Arpita Singh, et. al. International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 13, Issue 1, January 2023, pp. 157-165

RESEARCH ARTICLE OPEN ACCESS

Cloud Computing: Risk and Challenges

Arpita Singh*, Mohd. Hamza**,Shelendra***,Sushmita Vishwakarma****
**(Department of Information Technology, Buddha Institute of Technology, Gorakhpur*
Email: arpitasingh9972@gmail.com)
*** (Department of Information Technology, Buddha Institute of Technology, Gorakhpur*
Email: rebelnaushi0011@gmail.com)
**** (Department of Information Technology, Buddha Institute of Technology, Gorakhpur*
Email: singhshelendra70@gmail.com)
*****(Department of Information Technology, Buddha Institute of Technology, Gorakhpur*
Email: 0008sushmita@gmail.com)

ABSTRACT
Computing is changing constantly, creating new hardware and software technologies, improving software, and optimizing business process. IT world is changing very fast, on daily basis new technologies are introduced. Nowadays cloud computing is the buzz word in IT industry. Cloud computing in its simplest form is a model for allocating compute and storage resources on demand. In practice, it offers a new way to provide the resources virtually to the users which significantly alters the cost structure. Cloud computing is the next stage in evolution of the internet, it provides the means through which everything from computing power to computing infrastructure, applications and business process – can be delivered to you as a service wherever and whenever you need them. But with the ease of accessing the resources and increasing demand of cloud computing also attracts the attention of hackers. Hence, cloud providers are becoming a bigger target of malicious attacks. As more and more information of individuals is being stored on cloud, concern about its security arises. In this paper we will talk about the issues and challenges faced in cloud computing in detail.
Keywords - Cloud Computing, Virtual Machines, Service Providers, Security, Internet.

Date of Submission: 11-01-2023 Date of acceptance: 27-01-2023

---

1. INTRODUCTION

Many people are interested in learning more about cloud computing and how it functions. For Example: When travelling by bus or train, the greatest illustration to grasp is when you buy a ticket to your destination and hold bade to your seat until you arrive. Other passengers, like you, buy tickets and travel on the same bus as you, and it doesn't affect you where they go. When the bus arrives at your stop, get off. Cloud computing is similar to a bus in that it transports data and information for a variety of users while also allowing them to use its services at a low cost. It is a model for delivering information services that provides flexibility, scalability and facilities management to the cloud users so that they can perform their task easily [1]. Providers like Google, Amazon Web Service (AWS), Alibaba, Microsoft and IBM provide cloud-based services through for which user pay according to their need or can get access through annual subscription. The most common use of cloud that mostly every person who has phone uses is backup storage provided by Google Photos and Drives. Now the question arises why we need cloud computing? IT industry is changing day by day hence their requirement also changes very fast which results in popularity of cloud computing.IT industries don't want to spend on resources they simply rent the resources required from cloud which reduces the

cost

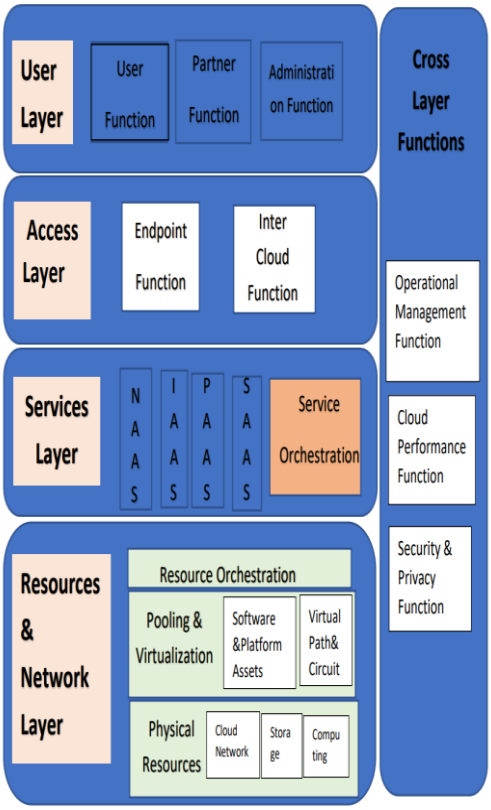

Fig. 1.1 components of cloud computing

1.1. Cloud Types

Clouds can be classified in terms of who owns and manages the cloud; a common destination is public clouds, private clouds, hybrid clouds and community clouds.[11]

1.1.1 Public Cloud

Public cloud or external cloud, is the most common form of cloud computing, in which services are made available to the general public in a pay-as-you-go manner. Customers or enterprises access these services over the internet from a third-party provider who may share computing resources with many customers. This model is widely accepted and adopted by Amazon, Microsoft and Google.

There are many benefits of deploying cloud as public cloud model: -

- Cost Effective
- Reliability
- Flexibility
- Location Independence
- Utility Style Costing
- High Scalability

1.1.2 Private Cloud

It is dedicated to a single customer and used when a proprietary network or data centre is operating solely for a business or organization, and serves customers within the business firewall. It is more secure than public cloud as no third party is involved.[12]

1.1.3 Hybrid Cloud

A hybrid cloud is a combination of two types of cloud, namely private and public, in which a private cloud can maintain high service availability by scaling up or increasing the range of their system with externally equipped resources from a public cloud when workload fluctuations or hardware breakdowns occur. A hybrid cloud allows an organisation to keep important data and applications inside the range of its firewall while hosting less critical ones on the public cloud.[25]

1.1.4 Community Cloud

The grid computing and volunteer computing concepts inspired the concept of community cloud. A community cloud allows several businesses with same service requirement can share infrastructure, boosting their scalability while lowering costs.[22]

1.2. Cloud Services

A cloud is a collection of systems that provide IT resources as a service to distant consumers. Hardware, development environments, and applications are all included in the resources. The following services are provided through cloud systems: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).[10]

1.2.1. Infrastructure as a service

The IaaS can be classified in two categories which are as follows- (1) Computation as a Service (CaaS) is a model in which servers based

in virtual machine are hired and charged per hour depending on the capacity of virtual machine, such as the Central Processing Unit and RAM size, as well as the virtual machine's features, operating system, and installed application software.[22]

(2) Data as a Service (DaaS) is a model in which a user's data is stored in an unlimited amount of space, independent of its kind, and the customer is charged per Gigabyte for data size and data transport. IaaS gives users access to basic resources like physical servers and machines, virtual machines and virtual storage.[26] Virtual machine backup or we can say disc storage, virtual LAN, network equipment, load balancers, IP addresses and software packages are all available through IaaS. Virtualization of servers makes all of these resources available to end users. Furthermore, customers access these resources as it is their own without any hinderance.

Some examples of IaaS services are: -

- GoGrid
- Amazon Simple Storage Services (S3)
- Rackspace Cloud
- Amazon Elastic Compute Cloud (EC2)

1.2.2. Platform as a Service

PaaS provides platforms and the environment on which the application services can run. The environment includes a pre-installed operating system, a platform such as interpreters or compilers for programming language that users may use to create and test applications on the platform. From the perspective of PaaS cloud users, computing resources are encapsulated into self-governing containers. This process is an alternative to virtualization known as containerization. These containers can develop their own applications using particular programming languages, and APIs are supported by the container. Using these containers, we need not to worry about resource management or allocation issues. Some examples of PaaS are: -

- Cloud Foundary from VMware
- Google App Engine
- AppFog
- Openshift
- Microsoft Azure
- Cloud Foundary from VMware
- SalesForce.com

1.2.3. Software as a Service

The popularity of SaaS is increasing day by day. SaaS uses the web to deliver applications that are managed by a third-party vendor and whose interface is accessible on the client side. SaaS applications can be run from a web browser without downloading or installing them, but they require a plugin. Cloud providers provide consumers with the ability to deploy applications on the cloud infrastructure. With this web provisioning model, SaaS eliminates the need to install and run applications on personal computers. In this model, companies can easily improve maintenance and support because everything can be managed by the vendors.[23] SaaS is based on subscribing software that are already present on a cloud platform for usage on demand. Traditional software usage is replaced with a subscribe/rent model, which lowers the user's requirements for physical equipments and operating cost.

Some examples of SaaS are: -

- Google Apps
- Salesforce
- Enoysion.com(Videomanagement)
- A2Zaps.com(Marketing Automation)

2. Advantages of Cloud Computing

- Pay-Per-Use Model or we can say only pay for what you utilize.
- Mobility means users may access information no matter where they are, rather than being reliant on infrastructure.
- Elasticity i.e., cloud resources can be scaled up or decreased depending on the need.
- Low maintenance cost.
- Versatile Compatibility i.e., it can be implemented on any platforms.

3. Cloud Computing Challenges

With growing influences of cloud computing it also becomes the center of attraction for hackers and

attackers. Some common challenges faced by cloud users are as follows: -

3.1. Data Protection

As cloud is used mostly for storage purpose, data security becomes a crucial element. Vendors must guarantee the protection of business data, but in many cases, the physical storage location of data is not known or disclosed to the users, adding to the security concerns of businesses. We can use firewalls or any IDS system across data centers to protect sensitive information in models which are previously used, but in the Cloud model, enterprises which provides the cloud services are responsible for data maintenance and security. As a result, cloud users must rely on cloud providers for data security.

3.2. Data Recovery and Availability

If someone saved their data on cloud it should be available when they need it and if a person is using cloud as a backup, then it will be the responsibility of cloud service providers to protect it from any damage. And if the data is damaged by mistake, then there must be a way of its recovery. Service level agreements between provider and users gives guarantee for the recovery and availability of data, and the enterprises are strictly adhered to this agreement. In the management of service level agreements and application runtime governance, operational teams are crucial. If a cloud provider fails to supply any of the given services, the consequences and possible repercussions could be severe**.**

- Fail over and proper clustering
- Keeping an eye on system
- Replica of the data
- Management of capacity and performance
- System and data maintenance (Runtime Governance)
- Disaster recovery

3.3. Management Capabilities: There are currently several cloud service providers, but platform and infrastructure management are still in its development phase. The scalability and load balancing technologies available now have a lot of room for improvement. If we wish to make improvements to our infrastructure or expand our storage capacity, it becomes a time-consuming operation. The scalability and load balancing technologies available now have a lot of room for improvement. If we wish to make improvements to our infrastructure or expand our storage capacity, it becomes a time-consuming operation. Enterprises providing cloud services must contain the property of auto scaling as it is an important or we can say a must have requirement but still many providers are not able to fulfil this requirement.

3.4. Interoperability and Flexibility

One platform's application should be able to use or integrate services from the other platform. Interoperability is the term used for this [19]. When a company utilizes a specific cloud service provider and wishes to migrate to another cloud-based solution, it can be a time-consuming process because applications created for one cloud must be rewritten for the other. Due to the complexity involved in migrating from one cloud to another, there is a lack of flexibility. Moving data, setting up security from scratch, and setting up a network are all challenges that come up when switching cloud providers, limiting flexibility.

4. Risks in using Cloud Computing

As day by day every enterprise is approaching virtualization hence they need a trustworthy platform for storing and retrieving data which should be efficient also. Currently opting cloud is the best option but with its efficiency comes lots of risks that can damage an enterprise reputation. We will discuss some of the risks faced in cloud computing as follows: -

4.1. Distributed Denial of Service

A Distributed DoS attack aims to overload website servers or increase the traffic by sending too many requests from different-different computers and preventing websites from responding the user who is in real need or to valid user requests. This can be done in the following ways given below: -

- With repeated requests, the demand on cloud services is drastically boosted.
- The network is overcrowded with traffic, causing it to become less responsive.

- Doing multiple works which require great amount of memory and time. Thus, exploiting as much possible resources.

Suppose there are two cloud service consumers A and B. Here A is an attacker in form of consumer and B is a legitimate service consumer. By submitting many requests, A now overloads the fundamental physical server's limit, resulting in blackouts on virtual servers A and B. As a result, legitimate customers are subjected to Denial-of-Service attacks.[15]

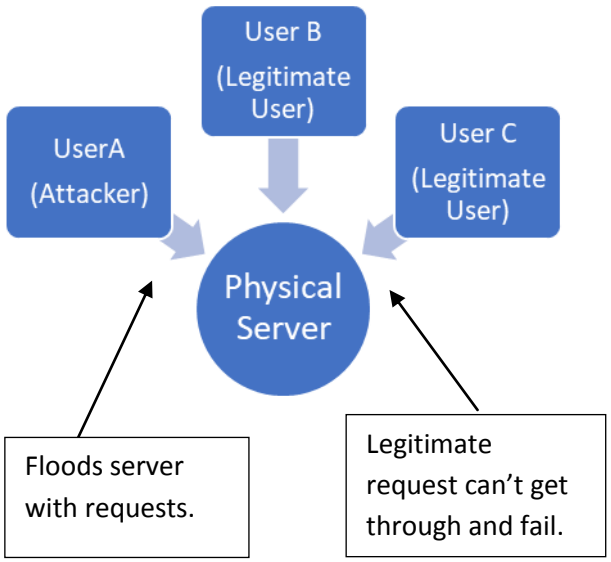

Fig. 1.2. DDoS Attack

A successful DDoS attack can make a website idle or of no use by decreasing its responsiveness for hours or even days. This can cause a decrease in revenue as well as a loss of customer trust and reputation of the cloud provider company. For businesses, adding DDoS protection to cloud services is now a necessary requirement**.**

4.2. Data Breaches

A data breach is a cyber-attack in which unauthorized person can access sensitive, confidential or otherwise protected data. On the cloud, data breaches have a higher risk of causing disaster and destruction. As general public mostly use cloud for backing up their important data which will be stored on cloud. But if the cloud service provider is not a trusted person then he/she will trade user's personal information for their own benefit with other enterprises. This happens mostly without the knowledge of cloud consumer. It happens when we get personalized advertisements on any website about which we didn't provide any information on that particular website.

Because some of these security measures are delegated to a trustworthy cloud partner (in all scenarios, including Private Cloud, Public Cloud, and Hybrid Cloud), cloud infrastructure can raise security concerns. Hence any flaw in cloud infrastructure must be avoided. A single weakness/flaw in a cloud service might turn a single data breach into a breach which can exploit the whole system. Various outcomes of data breach may include: -

- Brand name i.e., reputation of a famous company and trust of customers or partners or service providers can be compromised.
- Legal and Contractual Liabilities.
- The non-turbulant flow of intangible creation of the human intellect, the IP in the competitive sphere could severely damage the opening of product in the market.
- Change in laws and regulation could result in financial loss.

4.3. Traffic Eavesdropping

As the eavesdropping means knowing the information which are not meant for you. Similarly in cloud traffic eavesdropping happens when data being sent to or from a cloud is passively i.e., without the knowledge of sender and receiver intercepted by a malicious service agent with the goal of acquiring unauthorized information. Because of its passive nature, this form of attack can go undiscovered for long periods of time. This attack aims directly on compromising the confidentiality of the data.[20]

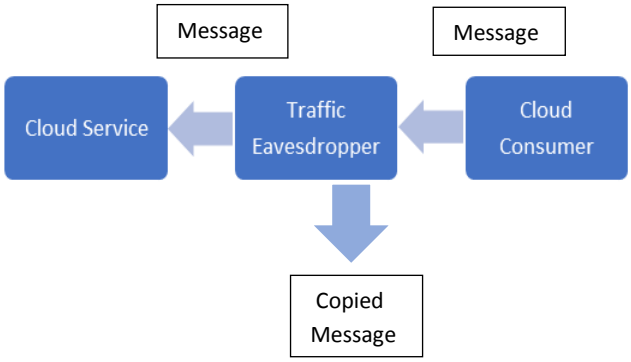

Fig. 1.3. Before the information is delivered on its way to the targeted host, the administrative specialist makes an unapproved copy of the information.

4.4. Hacked Interfaces and API Keys

On the cloud, API keys were initially used only as identifiers for client programs. While there were no security concerns at first, further advancements in cloud architecture have necessitated the usage of keys. These keys have been reported to be used for permission in some situations. As a result, owning this key grants you the ability to change, delete or transfer account data.[18]

Yahoo, Google and Amazon are all older and more experienced companies. Being experienced and trusted by the users still they have either fallen into this trap before or are aware of the flaws that exist. If API keys are going to secure information on the websites, then they need to be handled with greater care and responsibility. Application Program Interfaces or APIs are mostly used for connecting with cloud hence by hacking these interfaces any malicious person can access the data. According to University of Texas reports, some web services have weaknesses in the Secure Sockets Layer (SSL) protocol when accessed through APIs that aren't meant for a browser. These vulnerabilities in SSL can be used by attacker to gain unauthorized access. It was possible to gain access to a user's files by exploiting this weakness.[25]

4.5. Permanent Data Loss

Hackers can delete the data stored on cloud permanently by removing it from their real physical storage. All the data stored on cloud are stored somewhere physically either in distributed manner or at a single location. These physical locations are vulnerable to natural disasters. For cloud companies, adequate data backup and disaster recovery mechanisms are necessary. For instance, in 2011, Google was engaged in the deletion of approximately 1.5 million Gmail users' emails, contact information, and other information. Google employees spent their four days to fully recover the data of the affected customers after a software upgrade, according to Google.[6]

4.6. Overlapping Trust Boundaries

This type of risks arises in public cloud or hybrid cloud architecture. It is impossible to build a security architecture that spans such a trust border without introducing vulnerabilities. As every user on cloud can't be trusted but cloud provides same authorities to every user inside the trust boundary. It can be obtained only when cloud users and cloud providers use the same or similar security frameworks, which is unlikely with public clouds. Similar security frameworks can only be obtained in private clouds.

Because trust boundaries are merging and data is being exposed more widely, malevolent cloud consumers may have more possibilities to target IT systems and steal or harm corporate data.

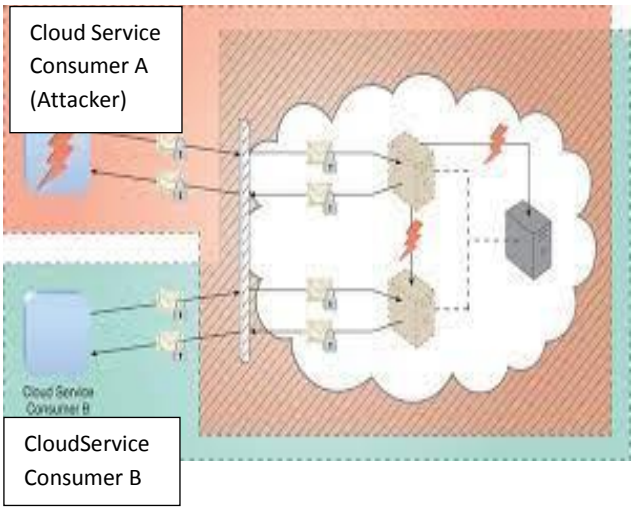

Fig. 1.4. illustrates that Two cloud service users A and B, share virtual servers hosted by the same physical server, and their trust boundaries overlap as a result.

In this Cloud consumer A can harm the virtual server and physical server as it is in the trust boundary, which is used by the B also. Thus, indirectly harming consumer B due to overlapped trust boundaries.

4.7. Virtualization Attack (VM Hopping)

Virtualization refers to the ability of a single physical machine, known as the host, to run numerous operating systems, known as virtual machines, at the same time. It gives various cloud users access to IT resources that share the same hardware resources but are logically separated from with each other. Work of one user doesn't affect the work of another user.[17]

When an attacker uses VM hopping, he or she takes control of one virtual machine and then tries to take control of another. This is a cloud security issue that occurs when someone gains access to your VIRTUAL MACHINE and host computer by hacking into the other virtual machine on the VMware server. It poses a significant risk because multiple VMs can run on the same host, making them all potential targets for the attacker.

4.8. Malicious Intermediary

Here the name itself suggesting that some malicious person intercepts in between the process and performs some unwanted person. Thus, it is a threat which occurs when messages are intercepted and manipulated by a malicious service agent, possibly jeopardizing the confidentiality and integrity of the message. This attack is similar to the Man in Middle attack. [1]

Attacker can also change the content of data or can insert harmful data before forwarding it to its destination

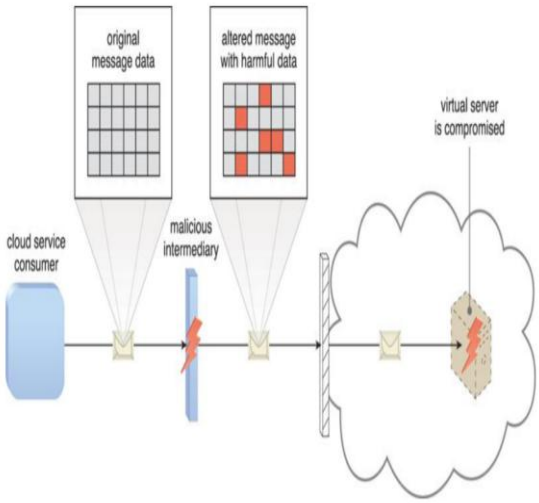

Fig. 1.5. Here the message is intercepted by an attacker and the content of data is changed. Since unsafe information is bundles into the message, the virtual server is traded off.

4.9. Insufficient Authorization

This attack occurs when access or unauthorized level of access are granted to an attacker in error. This can occur from weak authentication vulnerabilities related to weak passwords or shared accounts. Within cloud environments, these types of attacks can lead to significant impacts depending on the range of IT resources and the range of access to those IT resources the attacker gains. This attack is often a result of the attacker gaining direct access to IT resources that were implemented under the assumption that they would only be accessed by trusted consumer.

4.10. SQL Injection

This type of attack is directed towards trying to compromise or gain control over database and database servers. It commonly takes advantage of type of data being sent from a client to server. The attacker alters “injects” their own SQL commands into the data being sent to the server in order to get control over the server, or force the server to divulge data within database.[2]

5. REAL LIFE EXAMPLES

According to the Verizon Data Breach Investigations Report (DBIR), cloud security breaches have surpassed on prem-breaches for the first time. Below are some examples: -

5.1. YAHOO

It happened in August 2013 by a spear phishing mail, just one click and 3 billion accounts were affected. The company publicly announced it in December 2016. It's still the most devastating security breach.[3]

5.2. Alibaba

This took place in November 2019 and impacted more than 1.1 billion pieces of user data. Over an eight months period, a developer working for an affiliate marketers scraped customer data, including usernames and mobile numbers from the Alibaba Chinese shopping website, Taobao, using crawler software that he created. Hackers didn't get information about the encrypted data but the breach was severe enough.[4]

5.3. Sina Weibo

It happened in March 2020 and information like personal details including real name, username, gender, location and phone number of about 538 million Weibo accounts. The attacker obtained a part of Weibo database and sold to dark web in $250 as it doesn't include passwords.[4]

5.4. Target

Target security breach leaked approximately 70 million customer's credit card information during 2013. The attack was a result of network breach via an HVAC contractor monitoring store climate system, so once the Target system was breached, the hackers simply uploaded a grabber program to mirror payment data to Target server which was unused. Target losses approximately $400 million and customer's trust.[6]

6. Conclusion

As the cloud computing as its peak and every IT industry is shifting to cloud for being efficient and responsive to users. Hence it becomes most important provide a secure environment for the users to exchange their data on cloud. The security issues that were discussed in the research paper should be resolved and proper action should be taken against security breaches. As in present time data about anyone is precious thing which can be used to manipulate the users while surfing online or social media platform. From this paper we can say that a trusted cloud service provider is must and second most concerning issues are network breach and issues related to virtualization.

Acknowledgements

We thank all the people who have contributed in the development of our research.

References

[1]. Ashish Bhatnagar and Shailza Sharma, Cloud Computing (Scope, Challenges and Solutions)
[2]. OWASP Prevent SQL Injection, SQL Injection Prevention Cheat Sheet, (2016, May25). Retrieved from http://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet.
[3]. A blog named 7 most infamous Cloud Security Breaches on Storage Craft,(2022).Retrieved from https://blog.storagecraft.com/7-infamous-cloud-security-breaches/.
[4]. Michael Hill and Dan Swinhoe, The 15 biggest data breaches of the 21st century, (2022). Retrieved from https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.
[5]. John P. Mello Jr., 11 top cloud security threats, Journal of Engineering Science and Technology, 3(4), pp. 2672-2676, (2022). http://www.infoworld.com/article/3041078
[6]. Dhanamma Shankar Jagli, Cloud Computing and Security Issues, IJERA, 07(06):31-38 ,(2017)
[7]. NIST Definition of Cloud Computing, National Institute of Standards and Technology, (September 2011).
[8]. Definition of Hybrid Cloud, ATOS (apprenda),(5 January,2022).https://apprenda.com/library/glossary/hybrid-clouds-a-definition/
[9]. M. Armbrust, (2009), Above the clouds: A Berkley view of Cloud Computing, UC Berkeley EECS.

[10]. Myles Brown (May,2019) ,"What are four types of cloud computing services" ,ExitCertified . https://www.exitcertified.com/blog/4-cloud-computing-services on December 2021.
[11]. Bala Narayada Reddy G, Cloud computing-types of cloud,(2013). http://bigdatariding.blogspot.my/2013/10/cloudcomputingtypes-of-cloud.html .
[12]. B. R. Kandukuri, R. Paturi V and A. Rakshit, Cloud Security Issues,IEEE international conference on Services Computing.
[13]. Swapnil Saurav, The A to Z of Cloud Computing
[14]. John R. Vacca, Cloud Computing Security (Foundation and Challenges)
[15]. Rao Narendra, SrTadapaneni, Habeebullah Hussaini Syed, Cloud Computing Security and Challenges https://www.researchgate.net/publication/351528419_CLOUD_COMPUTING_SECURITY_CHALLENGES.
[16]. Keene C, The Keen View on Cloud Computing,(2009).
[17]. Virtualisation article retrieved from https://www.geeksforgeeks.org/virtualization-cloud-computing-types/ .
[18]. An article on RedHat," What is Virtualization?", (2018) https://www.redhat.com/en/topics/virtualization/what-is-virtualization .
[19]. A blog written by Jamie Juviler," What are API keys? (And are they secure?)" retrieved from https://blog.hubspot.com/website/api-keys .
[20]. Interoperability definition retrieved from https://www.omnisci.com/technical-glossary/interoperability .
[21]. Eavesdropping Attack Definition by Jake Frankenfield,(2020) retrieved from https://www.investopedia.com/terms/e/eavesdropping -attack.asp .
[22]. N. Ram, S. Tirupati and Dr.P.V.S., Deploying an Application on the Cloud, International Journal of Advanced Computer Science and Applications, (2011) https://www.researchgate.net/publication/274238598_Deploying_an_Application_on_the_Cloud .
[23]. Deba Prasaed Mozumder, Md. Julkar Nayeen Mahi and Md. Whaiduzzaman, Cloud computing security breaches and threat analysis, International Journal of Scientific and Engineering Research , (July 2017) https://www.researchgate.net/publication/320124329_Cloud_Computing_Security_Breaches_and_Threats_Analysis .
[24]. An article on zymitry.com,Security Threats to Cloud-based System, retrieved from https://zymitry.com/security-threats-cloud-based-systems/ .
[25]. Handbook on Cloud Computing from ebin.pub and retrieved from https://ebin.pub/handbook-of-cloud-computing-9781441965233-9781441965240-1441965238.html .
[26]. Subashini B., chapter 6 Secured Healthcare Data Analytics on the Cloud Using Blockchain Based Techniques, IGI Global retrieved from https://www.igi-global.com/chapter/secured-healthcare-data-analytics-on-the-cloud-using-blockchain-based-techniques/295224 .