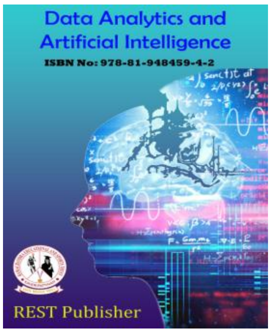
Data Analytics and Artificial Intelligence

Vol: 3(2), 2023

REST Publisher; ISBN: 978-81-948459-4-2

Website: http://restpublisher.com/book-series/daai/

DOI: https://doi.org/10.46632/daai/3/2/8



A Quick Review of Data Security, Privacy in Cloud Computing

J. Sathya

CMR University, Bengaluru, India.

*Corresponding Author Email: *sathya.j@cmr.edu.in*

Abstract*:* *Data security has been the major issue in information technology. People from all over the world put all kinds of information like public, private and confidential information in the cloud. Also data in the cloud are from various storage devices like servers, PC, mobile devices, smart phones and wireless sensor networks. So data security becomes a serious issue in the cloud environment. Protecting the data from unauthorized access is tedious. There are a lot of issues related to data security and privacy in cloud computing technology. This paper focuses on understanding the security and privacy issues in the cloud environment and comprehending compliance management in cloud computing.*

Keywords: *Cloud computing, Data Security, Data Privacy, Cloud Service Provider, Cloud Delivery Model, Cloud Deployment Model*

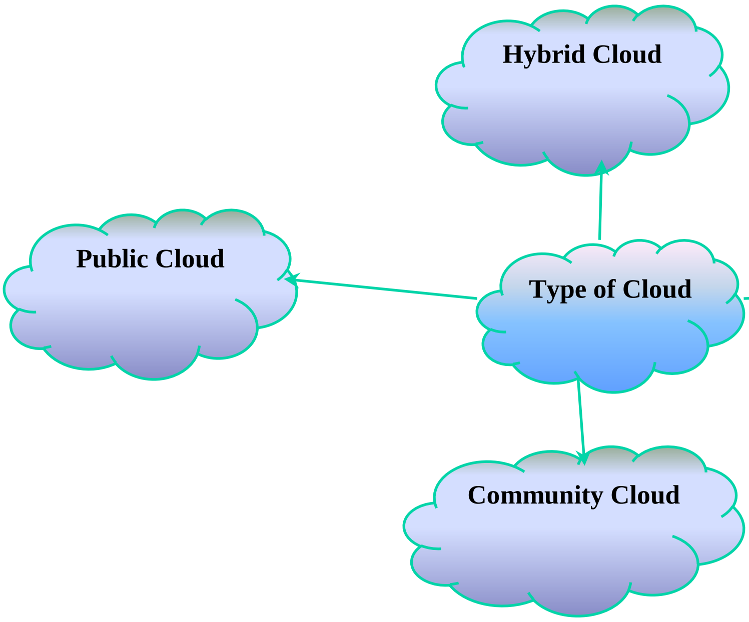
1. INTRODUCTION

Cloud computing is becoming the emerging trend in the field of computing. It is becoming popular by providing computing services like cloud storage, cloud hosting, and cloud servers etc. Cloud is an environment for hosting and delivering services over the internet. Cloud computing technologies such as Amazon's Elastic Computing Cloud (EC2), Simple Storage Service (S3) and Google App Engine have been the most popular in the software industry. Cloud computing provides a convenient on-demand network access to a shared pool of configurable computing resources. Resources refer to computing applications, network resources, platforms, software services, virtual servers, and computing infrastructure. Some issues like protecting data, preventing data loss, data leakage and various threats to the user's sensitive data on cloud storage need to be solved. To adopt any new technology, a trustworthy environment is the basic prerequisite. The security concern of the users and enterprises should be reformed by making the technology as trustworthy. The two main factors to gain user's confidence are data security and data protection. Various data security techniques have been proposed to protect the user data. In cloud computing Data security and Data privacy are two different and main factors which users have more concern. Both are according to hardware and software in cloud architecture. Data security in cloud computing is more cumbersome than traditional information systems.

2. DEPLOYMENT MODELS OF CLOUD

Deployment model specifies how resources are shared in the cloud. It is used for size, privacy and access. Cloud deployment types also represent the connections between the infrastructure and your users.[6] The four deploying models of cloud computing are:

Public Cloud: Small scale companies are adopting the public cloud. It is open and a good choice for development and testing teams. It is a great choice for companies with low-security concerns. Anybody can access systems and services easily. [10] It is less secure since it's open to everyone. This type of cloud is a good example for cloud hosting in which service providers supply services to a variety of customers. In this type storage backup and retrieval services are given for free, as a subscription, or on a per-user basis. [11] Example: Google App Engine



Benefits of Public Cloud

- *No Maintenance:* Does not cost you any maintenance charges as the service provider does it.
- *No Limit:* Does not have any limit on the number of users.
- *Infrastructure Management is not required:* Using the public cloud does not necessitate infrastructure management.
- *Infrastructure Management is not required:* Using the public cloud does not necessitate infrastructure management.

Limitations of Public Cloud

- *Less secure:* Public cloud is less secure as resources are public so there is no guarantee of high-level security.
- *Low customization**:*** It is accessed by many public so it can’t be customized according to personal requirements.

Private Cloud: Private cloud (also known as an internal cloud or corporate cloud) is managed by the organization or a third party. Only the authorized users can access the services from the provider. An organization which wants to make their customer data private will create a private data center to store the data. It is vulnerable incase of internal data theft and natural disaster. [6] It can also be managed and operated by a third party as in Public cloud. Most of the organization's choice is private cloud because it protects data in a better way. It can also be hosted on an independent cloud provider’s infrastructure. Some examples of private cloud vendors are AWS, Cisco, Google, Microsoft, Oracle, and IBM..,.

Benefits of Private cloud

- Good control over hardware and software.
- Personalize the hardware and software in any way
- Services run behind the customer’s own firewall provides Greater visibility into security and access control
- Has more control over its resources, information, and hardware than public cloud.

Disadvantages of Private Cloud

- Cost of purchasing and installing new hardware and software and the cost of managing is high
- Upgrading is more expensive - Once the hardware and software is installed adding capacity or new capabilities requires additional purchase
- Users of hosted deployment needs to subscribe and pay regularly for the offered service

Hybrid Cloud: Hybrid cloud refers to the combination of two or more computing environments such as public cloud, private cloud and community cloud. [6] It offers workload portability in such a way that applications work across different environments and communicate with multiple clouds. It is also possible to move the workloads between environments.

Benefits of Hybrid cloud

- Offers increased control over data.
- Provides the business with multiple options
- Requires much less space on-premises compared to a private model
- Unlimited due to on-demand cloud resources.

Disadvantages of Hybrid Cloud

- Customer does not know where the data is operating. So less control over data security.
- Networking becomes complex because of the integration of public and private clouds.
- Reliability of the services depends on cloud service providers.

Community Cloud: Community cloud enables different organizations to work on a shared platform. It allows multiple customers to work on joint projects and applications that belong to the community. It is also referred as a distributed infrastructure which integrates the services provided by different types of cloud infrastructure. Community clouds are more expensive than public clouds but also more secure. It's spread over in rowing organizations in the health, financial, legal, and educational sectors. [6] Key components of community cloud architecture are shared policies and protocols, cloud management systems, identity and access management system and shared application services. Some of the bodies which use community now are the U.S. Defense Department, 11.8% of universities in Turkey running community cloud architecture, and the healthcare industry in the U.S.

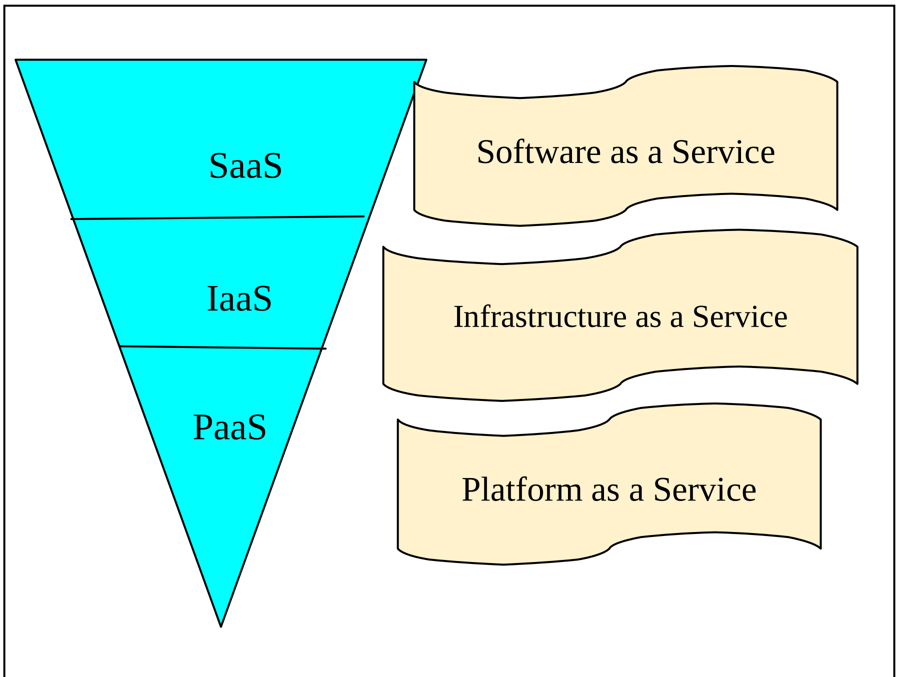
Benefits of community cloud

- Flexible to modify properties according to their individual use cases
- scalable in different facets such as hardware resources, services, and manpower
- Ensures the availability of data and applications at all times
- Users can configure various levels of security for their data

Challenges in community cloud

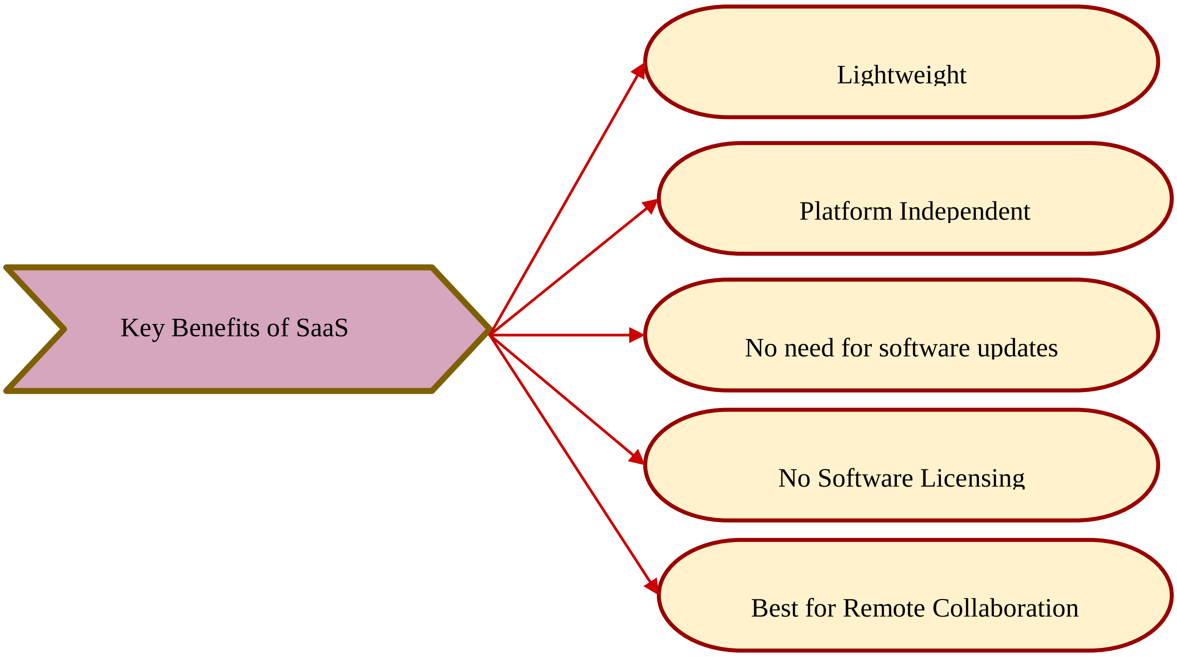
- Multiple organizations are accessing the data and involved in controlling the infrastructure of the community cloud. So security considerations will arise.
- All the participants in the community cloud have authorized access to the data. so organization must make sure not to share restricted data.
- Maintenance cost is high.

Delivery models of Cloud

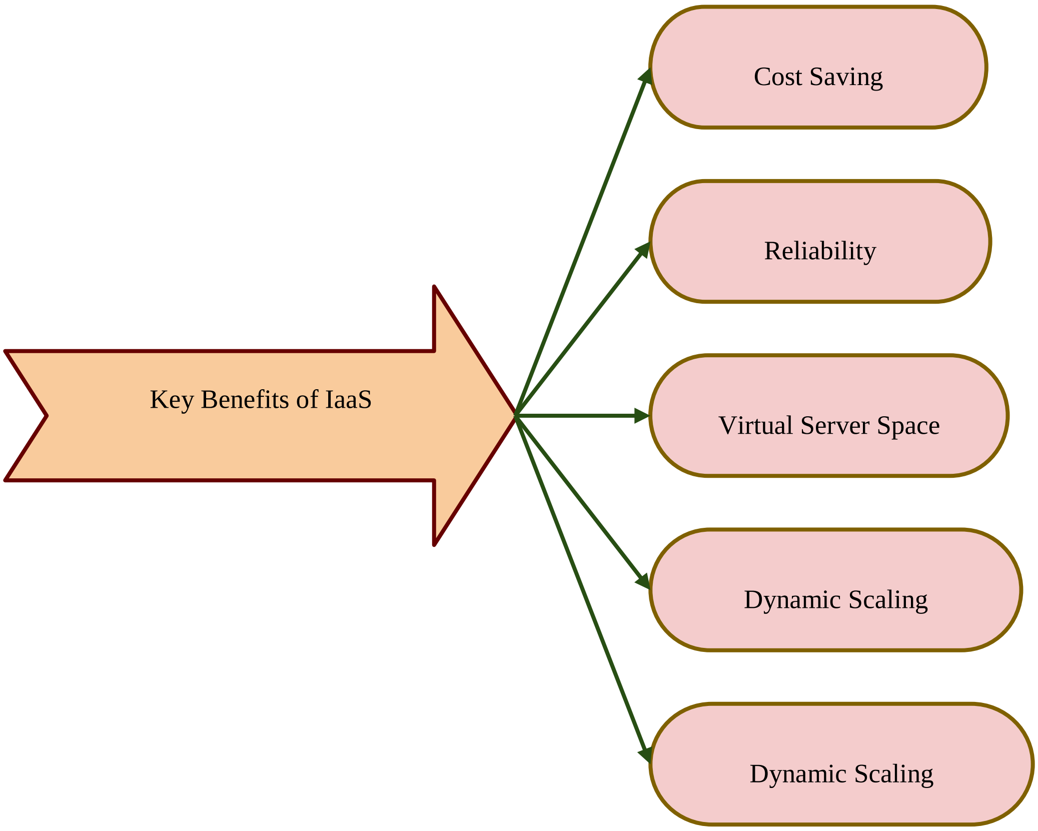


Delivery Models of Cloud Computing

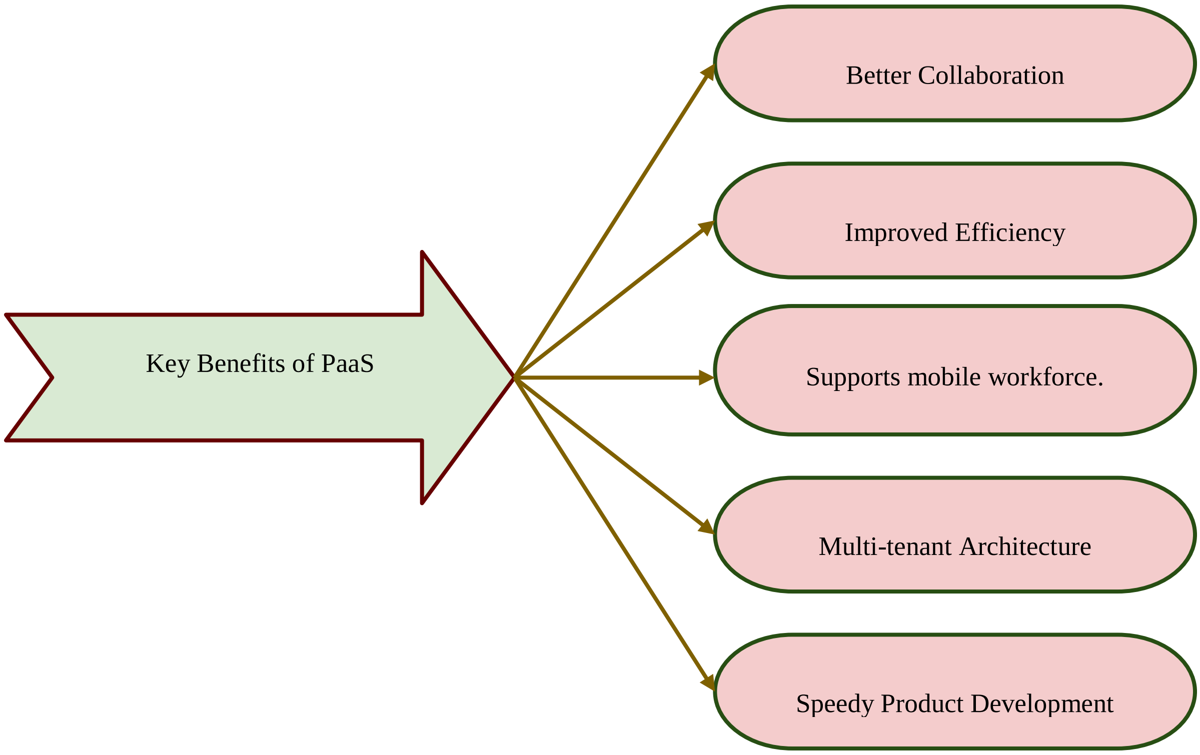
Software as a Service (SaaS): Software as a Service (SaaS) is a well-known delivery model and fully functional software which is run and administered by a cloud service provider/vendor. Its main purpose is to reduce the total cost of hardware and software development, maintenance, and operations. It is referred as is the superset of both, PaaS and IaaS. Because it offers the entire package from infrastructure, middleware, OS to applications deployed over the web.[1]



Infrastructure as a Service (IaaS): Infrastructure-as-a-service (IaaS) is the most manageable cloud computing service model which presents the required infrastructure and all the computing resources to users in a remote environment. As permits businesses to access virtualized computing resources from cloud servers. [18]It is the basic computing infrastructure of servers which provides on-demand service. It's main purpose is to avoid managing the hardware and software components, whereby all resources are obtained from other service environments.[1]

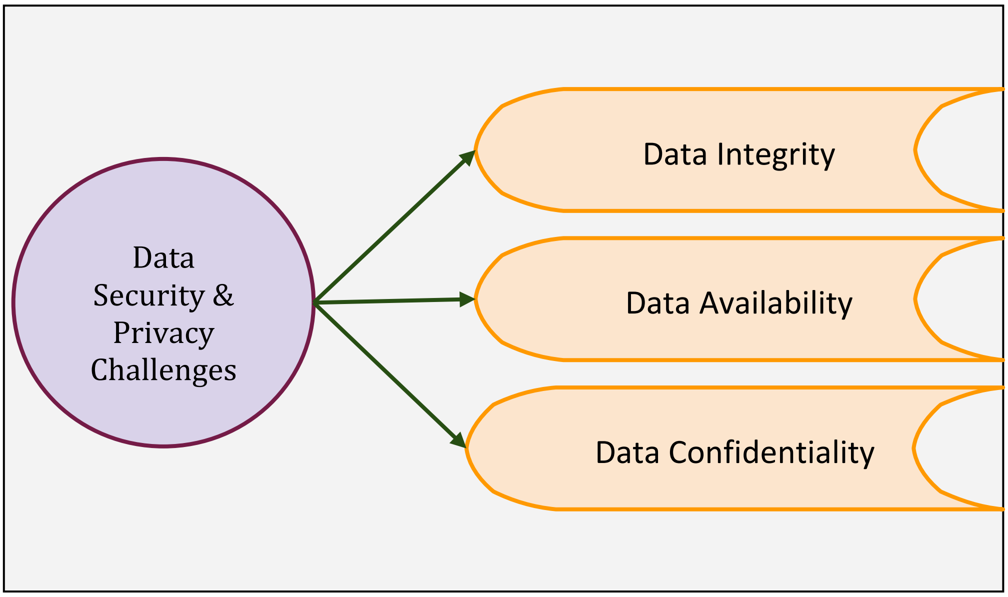


Platform as a Service (PaaS): Platform as a Service (PaaS) cloud service delivery model is a subset of SaaS which allows organizations to create, run, and manage cloud-based software without the need for onsite infrastructure.[18]It is also built on virtually but in the same infrastructure as IaaS.All services like DBMS, OS, Web servers are encapsulated in remote environment where users can use all without requiring any internal hardware and software.[1]


Key Benefits of PaaS
Better Collaboration
Improved Efficiency
Supports mobile workforce.
Multi-tenant Architecture
Speedy Product Development

3. DATA SECURITY AND DATA PRIVACY CHALLENGES

Data security within cloud computing is more complicated than data security within the traditional information systems. As we all know data protection is the protection of data from unauthorized access.[12] Data security becomes hazardous within the cloud computing environment, because data is disperse in different machines and storage devices including servers, PCs, and various mobile devices like wireless sensor networks and smart phones. [8]



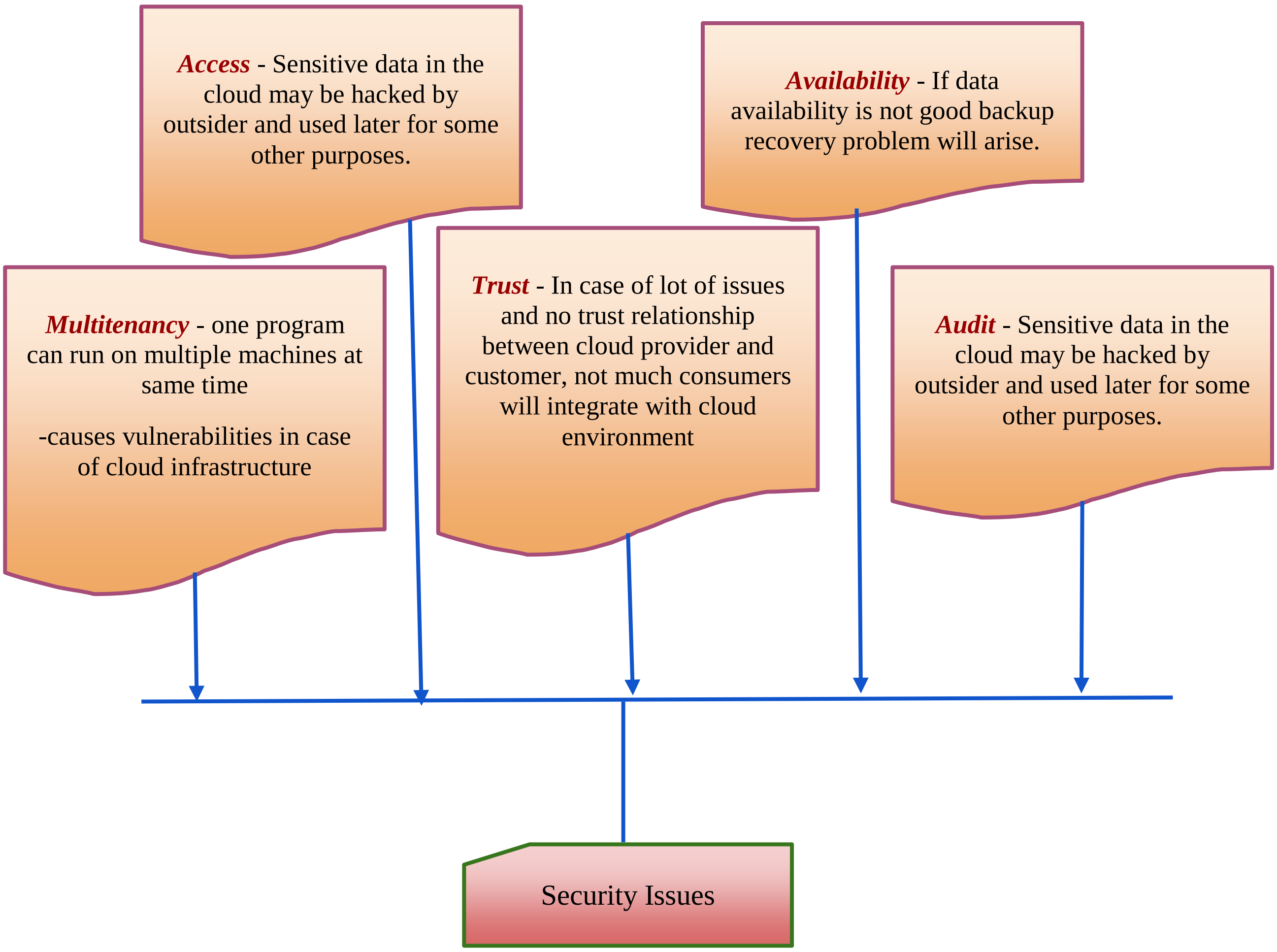
Data Integrity: Data integrity is the cornerstone to provide cloud computing services such as SaaS, PaaS, and IaaS. Besides data storage of large-scaled data, cloud computing environment usually provides data processing service. [2] Data integrity can be obtained by techniques such as RAID-like strategies and digital signature.

Data Confidentiality: Data confidentiality is ensured by authentication and access control strategies.[9] It is impossible for the cloud storage service providers to eliminate the insider threats virtually.[13]So it's not advisable to the user to store their sensitive data in cloud storage.[2]To ensure the confidentiality of data some of the security methods are used in cloud computing such as Homomorphic Encryption, Encrypted Search and Database, Distributive Storage and Hybrid Technique (uses both key sharing and authentication techniques)

Data Availability: Data availability whatever the data user stores so it should be available to that user at anytime and anywhere. The cloud vendors are governed by the local laws, so the cloud clients should be aware of those laws.[2]To acquire the trust relationship between the service provider and client, the cloud provider should share all such concerns with the client. Cloud storage provides the transparent storage service to decrease the control ability on data storage of users. [8]

4. SECURITY AND PRIVACY ISSUES IN CLOUD COMPUTING

This section describes the security and privacy related issues in the cloud environment. Data security comprises encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. To protect the data cryptographic mechanism is the best option. Both hardware encryption and software encryption techniques are suggested for the cloud. Data Integrity and data authentication ensures where the data is delivered. In addition, strong authentication is required for cloud deployment.[4] The trusted computing group's (TCG's) IF-MAP (Metadata Access Protocol) 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.[14]


Access - Sensitive data in the cloud may be hacked by outsider and used later for some other purposes.
Availability - If data availability is not good backup recovery problem will arise.
Multitenancy - one program can run on multiple machines at same time
-causes vulnerabilities in case of cloud infrastructure
Trust - In case of lot of issues and no trust relationship between cloud provider and customer, not much consumers will integrate with cloud environment
Audit - Sensitive data in the cloud may be hacked by outsider and used later for some other purposes.
Security Issues

5. TYPES OF ATTACKERS IN CLOUD COMPUTING

Internal Attacke

- Employed by the service provider, customers, or third-parties of cloud
- May have existing access to cloud services
- Uses existing privileges to gain further access for executing attacks against the confidentiality integrity and availability of information within the cloud service.

External Attacker

- Not employed by the service provider, customers, or third-parties
- Has no authorized access to cloud services, customer data or supporting infrastructure and applications
- Exploits technical, operational, process and social engineering vulnerabilities to attack a cloud service provider, customer or third party supporting organization to gain further access to propagate attacks against the confidentiality, integrity and availability of information within the cloud service.

Cloud Security Threats: The threats to information in the cloud can vary according to the cloud delivery models used by cloud user organizations. Some of the major threats are listed below

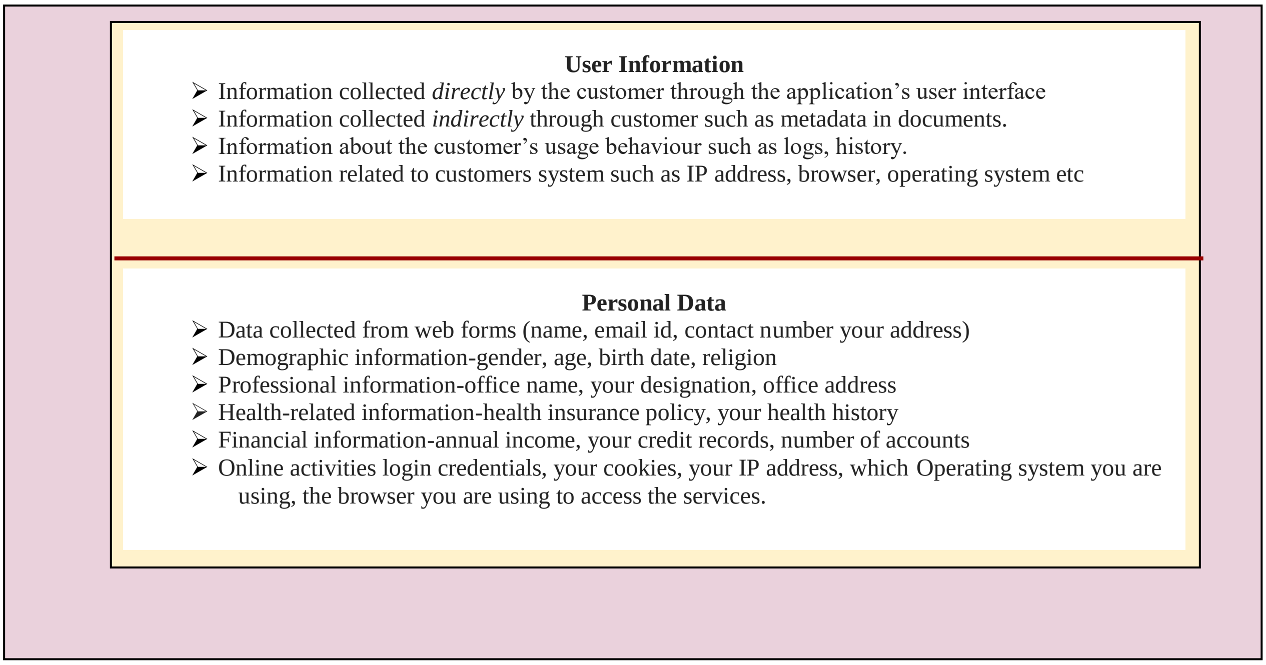
- Insider user threats
- External attacker threats
- Data leakage - Failure of security access rights across multiple domains
- Data segregation - Incorrect configuration of virtual machines and hypervisors
- User access - Poor identity and access management procedures
- Change management - Infrastructure changes upon cloud provider, customer and third-party systems impacting cloud customers.
- Physical disruption - Disruption of cloud provider, customer IT services through physical access

Data Privacy in Cloud Computing

Definition: Data privacy defines that your sensitive or confidential data on the internet is neither observed nor disseminated by other people. With data privacy, you can share data while protecting your personal data. There are millions of users' places available in private, public and community clouds. Several cloud customers don't even have knowledge of the physical location of the server where the data is being stored and how the information is processed on those servers. Cloud provides easy access of data similarly no control over data. [5]

PII (Personally Identifiable Information)-The personal information helps in uniquely identifying or locate a particular individual. This information can also be used with other resources to identify an individual. [17] The data collected from cloud is basically divided into two varieties:

- User Information
- Personal Data



User Information

- Information collected *directly* by the customer through the application's user interface
- Information collected *indirectly* through customer such as metadata in documents.
- Information about the customer's usage behaviour such as logs, history.
- Information related to customers system such as IP address, browser, operating system etc

Personal Data

- Data collected from web forms (name, email id, contact number your address)
- Demographic information-gender, age, birth date, religion
- Professional information-office name, your designation, office address
- Health-related information-health insurance policy, your health history
- Financial information-annual income, your credit records, number of accounts
- Online activities login credentials, your cookies, your IP address, which Operating system you are using, the browser you are using to access the services.

Challenges in Data Privacy

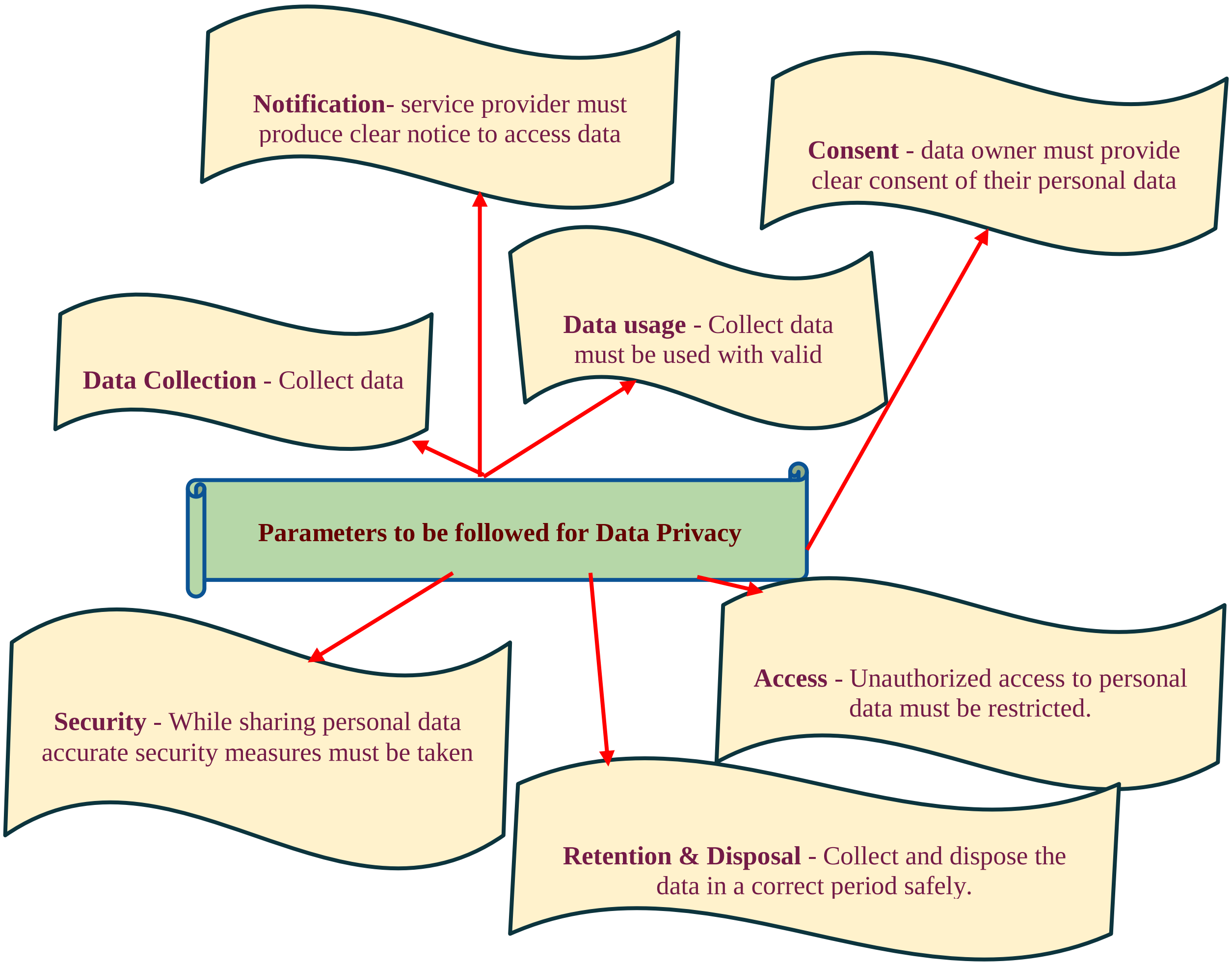
Complication in Assessing Risk - The risk to the privacy of data can be

- *Data Replication:* To maintain the redundancy of data, the cloud provider takes data backup periodically.
- *Data Loss:* In the cloud, it is easier to lose data. So the cloud customer must ensure that all the users must access the cloud data within a predefined policy and must have authority to block the user violating the policy.

Implying Consumer Privacy in Emerging Business Model: Cloud services enable the users to collect, store and share a vast amount of data at a very low cost. Increasing users also increases the risk. The emerging business model collects consumer data over a time, at a specific level; they also collect user's profile data. This collection of consumer data does not have consent with the privacy of consumer's data and even is unknown to the consumer.

Internal Threat: You might store your data at a safer place in a cloud environment. But your company employees who have access to data over the cloud can misuse their authorization to access the crucial information of the company such as financial information, customers details etc.[6]

Protecting Data Privacy: To protect the privacy of data FTC (Federal Trade Commission) has pointed out a few parameters that are discussed as below:


Notification- service provider must produce clear notice to access data
Consent - data owner must provide clear consent of their personal data
Data usage - Collect data must be used with valid
Data Collection - Collect data
Parameters to be followed for Data Privacy
Access - Unauthorized access to personal data must be restricted.
Security - While sharing personal data accurate security measures must be taken
Retention & Disposal - Collect and dispose the data in a correct period safely.

Best Practices for Data Security in cloud computing: Opting the right cloud service provider will minimize the security problems. A good vendor knows the importance of protection of data. Below are some key factors consumers can look into before choosing a cloud.[3] *Controls available to prevent data* - built-in secure cloud computing controls that help to prevent issues such as unauthorized access, accidental data leakage, and data theft. Some questions consumers can ask the service provider.

- Are permission settings granular enough?
- Is it reliable enough?
- Are intuitive enough for internal users to share content with external partners?

Well-built Authentication: Make sure your CSP offers strong authentication measures to ensure proper access through strong password controls and multi-factor authentication (MFA). The CSP should also support MFA for both internal and external users and single sign-on, so users can just log in once and access the tools they need.[19]

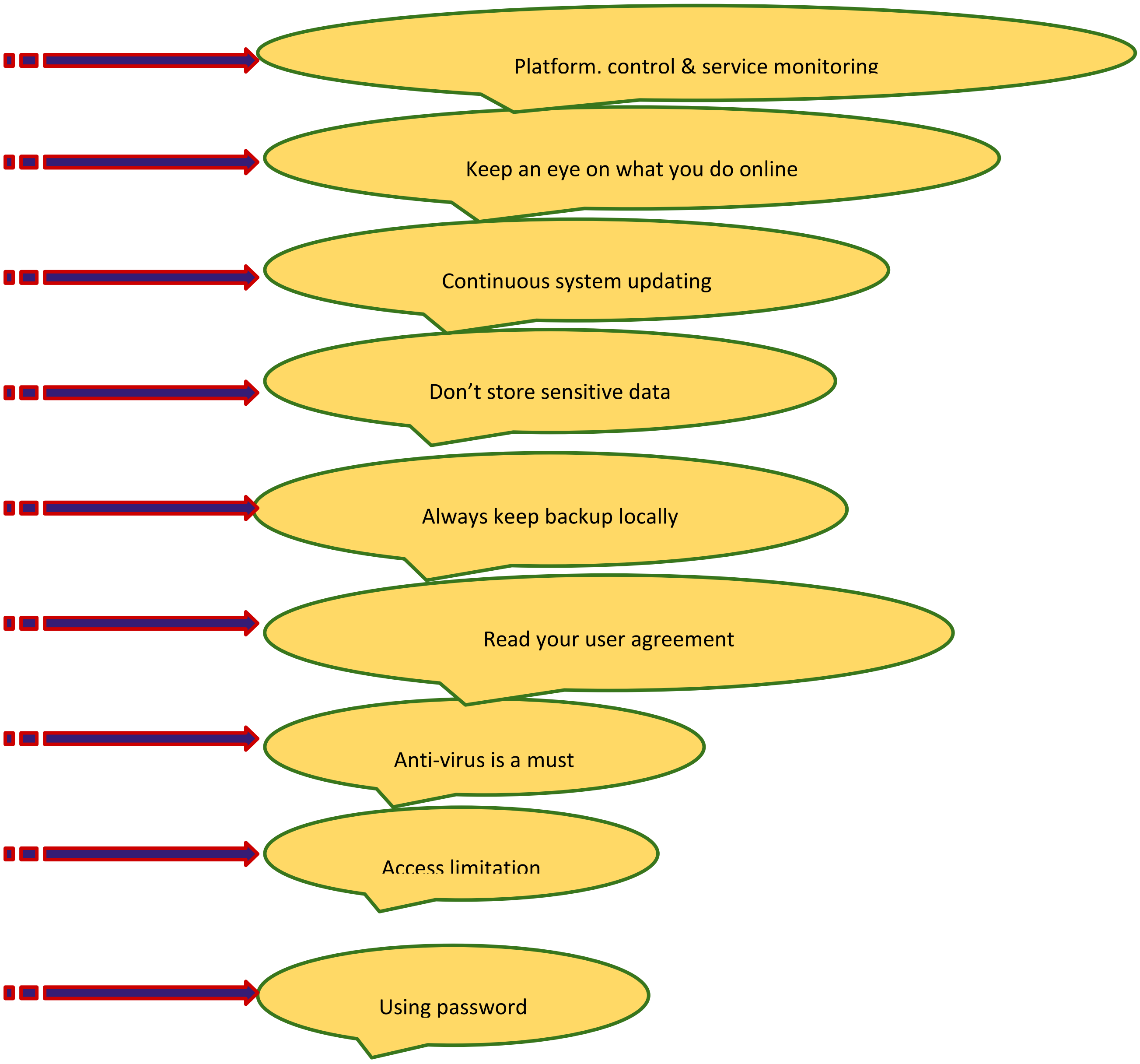
Data Encryption: Ensure that all data is encrypted at both rest and in transit. Cryptographic encryption technique use symmetric key encryption at rest to encrypt the data.[15]Data is encrypted in transit across wireless or wired networks by transporting over a secure channel using Transport Layer Security(TLS).Best Cloud environment allows customers to manage their own encryption keys without diminishing user experience.

Visibility and threat detection: Secure cloud service provider allows administrators to have a view of all user activity and all internally and externally shared content. It uses machine learning algorithms to analyze usage to learn patterns of typical use, and then they look for cases that fall outside those norms. And also alerts will be generated when suspicious activity is detected.

Continuous compliance: A provider that focuses on continuous compliance can protect your company from legal troubles and ensure you're using the most updated security practices.[19]

Integrated security - check to see if the provider’s tools easily integrate with your security stack through representational state transfer architectural style APIs.

Apart from the above-mentioned practices consumers put some extra effort to protect their data from unauthorized access. [16]


Platform. control & service monitoring
Keep an eye on what you do online
Continuous system updating
Don’t store sensitive data
Always keep backup locally
Read your user agreement
Anti-virus is a must
Access limitation
Using password

6. CONCLUSION

In this paper we have started with cloud definition, importance of cloud computing, deployment models, delivery models, need for data security, some security and privacy attributes, Common methods to protect personal data. Cloud computing is a promising and emerging technology for the next generation of IT applications. Barriers and hurdles will come when we deal with data accessing. Several techniques have been proposed by researchers for data protection and to attain the highest level of data security in the cloud. Public cloud is open, risks and threats of data loss or theft increases. Private cloud and other types also not fully secured but comparing to public cloud data privacy is little higher. Many techniques are proposing by researches to avoid the security issues and to achieve the highest level of data security. Still cloud is a cross over environment, vulnerabilities will arise. Consumer must select the right CSP and to avoid sharing personal and more confidential data.

REFERENCES

[1]. Jaydip Sen, Security and Security andPrivacy Privacy Privacy Issues in Cloud Computing, Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA

[2]. Yunchuan Sun, Junsheng Zhang,Yongping Xiong,and Guangyu Zhu,Data Security and Privacy in Cloud Computing , Hindawi Publishing Corporation,International Journal of Distributed Sensor Networks Volume 2014, Article ID 190903,2014

[3]. Yunusa Simpa Abdulsalam and Mustapha Hedabou,Security and Privacy in Cloud Computing: Technical Review,DNA Lab, School of Computer and Communication Science, University Mohammed VI Polytechnic,2021

[4]. Mahesh U. Shankarwar and Ambika V. Pawar,Security and Privacy in Cloud Computing: A Survey, CSE Department, SIT, Symbiosis International University, Pune, India,2014

[5]. Sugandh Bhatia, Jyoteesh Malhotra,CSPCR: Cloud Security, Privacy and Compliance Readiness - A Trustworthy Framework, International Journal of Electrical and Computer Engineering (IJECE),Vol. 8, No. 5, pp. 3756~3766,ISSN: 2088-8708, October 2018

[6]. Ahtisham Hashmi, Aarushi Ranjan, Abhineet Anand,Security and Compliance Management in Cloud Computing, INTERNATIONAL JOURNAL OF ADVANCED STUDIES IN COMPUTER SCIENCE AND ENGINEERING IJASCSE VOLUME 7, ISSUE 1, 2018

[7]. Zhifeng Xiao and Yang Xiao, Senior Member, IEEE,Security and Privacy in Cloud Computing,IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 2, SECOND QUARTER, 2013

[8]. Yunchuan Sun, Junsheng Zhang and Guangyu Zhu,Data Security and Privacy in Cloud Computing , SAGE Journals,2014

[9]. Pierangela Samarati, Data Security and Privacy in the Cloud, ebook, ISBN: 978-3-319-06320-1, Part of the Lecture Notes in Computer Science book series (LNSC,volume 8434), 2014

[10]. Giulio D'Agostino, Data Security in Cloud Computing, Volume I Kindle Edition, ISBN-13 978-1947083998, Publisher:Momentum Press,2019

[11]. Tim Mather, Subra Kumaraswamy, and Shahed Latif, Cloud Security and Privacy, First edition, Published by O’Reilly Media, Inc.,2009

[12]. Wei Ren ; Lizhe Wang ; Kim-Kwang Raymond Choo ; Fatos Xhafa, Security and Privacy for Big Data, Cloud Computing and Applications, ISBN: 9781785617478,2019

[13]. Giulio D'Agostino, Data Security in Cloud Computing, Volume I, Publisher Momentum Press, ISBN 9781949449006,2019

[14]. Elisa Bertino, Data Security – Challenges and Research Opportunities, Research Paper, Springer International Publishing , Switzerland 2014

[15]. Venkata Sravan Kumar Maddineni ,Shiva shanker Ragi, Security Techniques for Protecting Data in Cloud Computing, Master Thesis , Electrical Engineering, November 2011

[16]. https://www.apogaeis.com/blog/data-privacy-security-in-cloud-computing/

[17]. https://binaryterms.com/data-privacy-in-cloud-computing.html

[18]. J.M.Suri, DDG(I), TEC, B.K.Nath, Dir(I), TEC, Security and Privacy in Cloud Computing, Telecommunication Engineering Centre, Khurshid Lal Bhawan, Janpath, New Delhi

[19]. https://www.box.com/en-in/resources/what-is-cloud-security