5.1 Trust in Cloud

Trust means Assurance, Confidence, in data, processes, and people. First question before moving to the cloud, "How let our data flow over networks, through organizations, and to devices outside of our infrastructure, between an exponentially increasing number of providers, without losing control and security? [33].

5.1.1 Security isn't the issue, trust is

Cloud computing doesn't need to be a threat to IT security; it can actually be part of the solution. The abstraction layer that cloud computing creates can actually improve visibility, a fundamental requirement for effective security [33]. The challenge arises from lack of ownership and the corresponding concerns over lack of control [33]:

- **Infrastructure:**

  How to ensure that the infrastructure providers have appropriate security and disaster recovery policies and stick to them?

- **Identity:**

  How to enforce rigorous authentication across multiple interconnected systems without adversely affecting flexibility and productivity?

- **Information:**

  How to classify and protect sensitive information, and ensure compliance with policies and regulations?

5.1.2 Trust in Data Center

To gaining the advantages of cloud computing in the enterprise begins with establishing a trusted approach to the cloud [34].

Trust in a cloud data center centers on several core concepts [34]:

- Security: Traditional issues around data and resource access control, encryption, and incident detection are factors here.
- Control: The ability of the enterprise to directly manage how and where data and applications are deployed and used.
- Compliance and service-level management (SLA): This concept refers to contracting and enforcement of service-level agreements between varieties of

parties, and conformance with regulatory, legal, and general industry requirements.

So Security and privacy concerns are among the top concerns standing in the way of wider adoption of cloud. In cloud computing the main concern is to provide the security to end user to protect files or data from unauthorized user [35].

5.2 Security concern

Culture and comfort aside, simply communicating data over the public internet, as opposed to keeping it entirely within a private corporate network, may increase data vulnerability. In addition, the business models of Cloud Service Providers (CSPs) involve sharing infrastructure among many clients and managing IT workloads among many different physical machines or even geographically dispersed data centers [36].

Cloud Computing reduces cost by sharing computing and storage resources, merged with an on demand provisioning mechanism relying on a pay-per use business model. Due to varied degree of security features and management schemes within the cloud entities security in the cloud is challenging [37].

Security issues ranging from system miss-configuration, lack of proper updates, or unwise user behavior from remote data storage that can expose user's private data and information to unwanted access can plague a Cloud Computing [37].

5.2.1 Security Issues

Cloud is expected to offer the capabilities like encryption strategies to ensure safe data storage environment, strict access control, secure and stable backup of user data. However, cloud allows users to achieve the power of computing which beats their own physical domain. It leads to many security problems. The major security concerns are [37]:

- **Identification and Authentication**: The multi tenancy in cloud computing allows a single instance of the software to be accessed by more than one users. This will

cause identification and authentication problem because different users use different tokens and protocols that may cause interpretability problems [37].

- **Access control**: Confidential data can be illegally accessed due to lenient access control. If adequate security mechanisms are not applied then unauthorized access may exist. As data exists for a long time in a cloud, the higher the risk of illegal access [37].
- **Data Seizure**: The Company providing service may violate the law. There is a risk of data seizure by the some foreign government [37].
- **Encryption/ Decryption**: There is an issue of the Encryption/ Decryption key that are provided. The keys should be provided by the customer itself [37].
- **Policy Integration**: Different cloud servers can use different tools to ensure the security of client data. So integration policy is one of the major concerns of security [37].
- **Audit**: In cloud computing the Cloud Service Provider (CSP) controls the data being processed. CSP may use data while being processed. So the process must be audited. The all user activities must be traceable. The amount of data in Cloud Computing may be very large. So it is not possible to audit everything [37].
- **Availability**: Availability is the major concern in the cloud computing. When the client data is virtualized, clients have no control on the physical data. If in the cloud, the data or service is not available, it is rigid to fetch the data [37].
- **Network Consideration**: Cloud computing is a technique of resource sharing where servers and storage in multiple locations are connected by networks to create a pool of resources. When applications are run, resources are allocated from this pool and connected to the user as needed. The missions of connecting the resources (servers and storage) into a resource pool and then connecting users to the correct resources create the network's mission in cloud computing. For many cloud computing applications, network performance will be the key to cloud computing performance [37].
- **Virtualization Paradigm**: In order to process a user request in cloud computing CC environment, a service provider can draw the necessary resources on demand, perform a specific job and then relinquish the unneeded resources and often

dispose them after the job is done. Contrary to traditional computing paradigms, in a cloud computing environment, data and the application is controlled by the service provider. This leads to a natural concern about data safety and also its protection from internal as well as external threats. Usually, in a cloud computing paradigm, data storage and computation are performed in a single data enter that may led to the development of various security related failure [37].

- **Mapping machines**: Cloud computing offers a means to decouple the application activities from the physical resources required. This has enabled consolidation of multiple applications onto a lesser number of physical servers resulting in an increase in server utilization. Such decoupling of resources is facilitated by the concept of a virtual machine which encapsulates an application with a specific set of functionalities. Physical resources are made available to the virtual machine by a guest operating system running on each physical machine. The virtual machine runs over this guest operating system which also provides facilities for creation, destruction and migration of virtual machines. The different security parameters are required to facilitate these functions in cloud computing [37].
- **Secure Data Management:** As data is an important tool of CC the some aspects of the secure cloud, namely aspects of the cloud storage and data layers. In particular the security issues ranging from ways of efficiently store the data in foreign machines to querying encrypted data, as much of the data on the cloud may be encrypted is a critical challenge for implementing security schemes in Cloud Computing [37].
- **Resource Allocation:** With the cloud model, we lose control over physical security. In a public cloud, we are sharing computing resources with other companies. In a shared pool outside the enterprise, we don't have any knowledge or control of where the resources run. Exposing our data in an environment shared with other companies could give the government "reasonable cause" to seize assets because another company has violated the law. Simply because we share the environment in the cloud, may put the data at risk of seizure. Storage services provided by one cloud vendor may be incompatible with another vendor's services

should decide to move from one to the other. Thus to secure the resources in a cloud demand highly encrypted schemes [37].

5.2.2 Security standard

- Ensuring that cloud computing occurs in a secure environment is a concern not only for users, but also for governments trying to facilitate the take-up of cloud [38].

5.3 Privacy & data protection

On the privacy side, there is the concern, of course, that personally identifiable information stored in the cloud can be breached more easily than if stored in-house — but that's mainly a security concern. Beyond data protection, the core privacy problem for enterprise businesses adopting cloud computing stems from the diversity of privacy regulations from country to country, alongside against the CSP business model [39].
Cloud providers should protect the assured, proper, and consistent collection, processing, communication, use and disposition of personal information (PI) and personally identifiable information (PII) in the cloud. PII is the information that can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Though cloud computing provides a flexible solution for shared resources, software and information, it also poses additional privacy challenges to consumers using the clouds [39].

In side of data protection, data must be secured while at rest, in transit, and in use, and access to the data must be controlled. Standards for communications protocols and public key certificates allow data transfers to be protected using cryptography. Procedures for protecting data at rest are not as well standardized, however, making interoperability an issue due to the predominance of proprietary systems. The lack of interoperability affects the availability of data and complicates the portability of applications and data between cloud providers [40].

5.3.1 Privacy challenges

Cloud computing, in which services are carried out on behalf of customers on hardware that the customers do not own or manage, is an increasingly fashionable business model. The input data for cloud services is uploaded by the user to the cloud, which means that they typically result in users' data being present in unencrypted form on a machine that the user does not own or control. This poses some inherent privacy challenges [44].
There is a risk of data theft from machines in the cloud by rogue employees of cloud service providers or by data thieves breaking into service providers' machines, or even by other customers' of the same service if there is inadequate separation of different customers data in a machine that they share in the cloud. Governments in the countries where the data is processed or stored may have legal rights to view the data under circumstances. There also a risk that the data may be put to unauthorized uses. It is part of the standard business model of cloud computing that the service provider may gain revenue from authorized secondary uses of the users' data, most commonly the targeting of advertisements. However, some secondary data uses would be very unwelcome to the data owner (such as, for example, the resale of detailed sales data to their competitors). At present, there are no technological barriers to such secondary uses. There are, however, some legal constraints on treatment of users' private data by cloud computing providers [44].

International agencies as well as national policy makers and regulators must work together to develop efficient, effective, proportionate and readily enforceable laws to protect consumers' reasonable expectation of privacy. Responsibility should also be devolved to stakeholders developing self-regulation, for example establishing privacy policies that are transparent and appropriate for the services they provide. Governments should also continue to work together to ensure no single entity adopts privacy regulations that are so burdensome that they restrict the free flow of information or prevent CSPs from maximizing the cost saving inherent in those services [42].

5.4 Intellectual Property Rights

In Europe, there is a Act entitles ISP accessing the content of the data and client systems to detect a violation of proprietary rights and intellectual property, and not causing defamation to preserve the others rights, so ISP have legal exonerating as intermediary detector [27].

5.5 Data Security Considerations

Public-cloud providers often have multiple data storage systems located in multiple data centers, which may often be in multiple countries or regions. Consequently, the client may not know the location of their data, or the data may exist in one or more of several locations at any particular time. Additionally, a client may have little or no visibility into the controls protecting their stored data. This can make validation of data security and access controls for a specific data set particularly challenging [43].

It is recommended that data-security needs are evaluated for all types of information being migrated to a cloud environment. For example, operational data, security policies and procedures, system configurations and build standards, log files, audit reports, authentication credentials, cryptographic keys, incident response plans, and employee contact details are just some of the types of data with different security requirements that may need to be considered. If data security processes are not clearly defined and documented, the data may be unintentionally exposed or subject to unnecessary risk that could result in loss or inappropriate disclosure [43].

5.5.1 Data storage and persistence

In addition to the known range of intended storage locations, data may also be present in other CSP systems used for maintenance of the cloud infrastructure, such as VM images, backups, monitoring logs, and so on. All potential capture points should be identified and managed as necessary to prevent unintended or unsecured storage or transmission of sensitive data. Specialized tools and processes may be needed to locate and manage data stored on archived, off-line, or relocated images [43].

5.5.2 Data lifecycle management

For all cloud models, clear requirements for data retention, storage and secure disposal should form an integral part of the engagement process to ensure that sensitive data is:

- Retained for as long as needed,
- Not retained any longer than needed,
- Stored only in appropriate and secured locations, Accessible only to those with a business need, and
- Handled in accordance with the client's security policy

Because all environments outside the client-controlled environment could potentially be un-trusted, cloud services should support the secure transmission of data throughout the cloud infrastructure, between the client and cloud environments, between client environments, and between the cloud infrastructure and other public networks. It is recommended that sensitive data be encrypted for all transmissions through any cloud environment that is not entirely private and/or controlled by the client. Cloud environments outside of the client-controlled environment should be treated as "open" or "public" networks [43].

In a distributed cloud environment, verifying that all instances of data have been securely deleted in accordance with the client's data-retention policy is subject to the same challenges identified for validating data security and access controls [43].

5.5.3 Data Classification

Data classification and the management of data according to its classification will vary from organization to organization. A defined data-classification system can help organizations identify data that is sensitive or confidential, and data with specific security needs. This in turn allows organizations to assign appropriate protection mechanisms based on the security needs of different data types, and helps to prevent sensitive data from being inadvertently mishandled or treated as non-sensitive [43].

Organizations should ensure that their particular data security needs can be met by the cloud service before migrating that data into the cloud environment. Considerations should include how storing data types with different levels of sensitivity in the same virtual environment may impact the protection levels required for each data type. User credentials and passwords, and cryptographic keys are examples of sensitive data that must be protected according to their individual needs [43].

5.5.4 Data Encryption and Cryptographic Key Management

In a public-cloud environment, one client's data is typically stored with data belonging to multiple other clients. This makes a public cloud an attractive target for attackers, as the potential gain may be greater than that to be attained from attacking a number of organizations individually. Strong data-level encryption should be enforced on all sensitive or potentially sensitive data stored in a public cloud. Because compromise of a CSP could result in unauthorized access to multiple data stores, it is recommended that cryptographic keys used to encrypt/decrypt sensitive data be stored and managed independently from the cloud service where the data is located. At a minimum, key-management servers should be located in a separate network segment and protected with separate access credentials from the VMs that are using the keys and the data encrypted with them [43].

Only defined, authorized key custodians should have access to cryptographic keys. Because access to both keys and encrypted data provides the ability to decrypt the data, clients will need to verify who has access to cryptographic keys, who has access to the encrypted data, and who has access to both. If a client shares encryption keys with the CSP, or engages the CSP as a key custodian, details of CSP access permissions and processes will also need to be reviewed and verified [43].

This consideration is particularly critical if cryptographic keys are stored or hosted by a third-party CSP that also hosts the encrypted data. If CSP personnel have access to a client's keys and the client's encrypted data, the client may have unintentionally granted the CSP ability to decrypt their sensitive data [43].

Any data that is decrypted in the cloud may be inadvertently captured in clear text in process memory or VMs via cloud maintenance functions (such as snapshots, backups, monitoring tools, etc.). To avoid this risk, clients may choose to keep all encryption/decryption operations and key management on their own premises, and use a public cloud only for storage of the encrypted data. Applicable controls must be applied to the encryption, decryption, and key-management processes to ensure data can only be retrieved (decrypted) by those who are authorized with a defined business need [40].

CSPs providing cryptographic-key management services for their clients should ensure that secret or private keys are not shared among clients—each client should be provided

with a unique key or set of keys. Secure channels for access to the cloud environment also require proper key management. If the CSP uses images or cloning for protecting VMs, it is strongly recommended that keys not be cloned as part of the VM image—each clone or VM instance should have its own key(s) [43].

5.5.5 Decommissioning and Disposal

In addition to data disposal, resource decommissioning requirements should be defined to support clients' future decisions to migrate to a new CSP, decommission their cloud resources, or move out of a cloud environment altogether. The CSP should provide data-disposal mechanisms that provide assurance to the client that all data has been securely removed and deleted from the cloud environment. Procedures for "termination of service" should be clearly defined and documented [40].

Clients may choose to ensure that all data is encrypted with strong cryptography to reduce the risk to any residual data left behind on CSP systems. However, clients should be aware that leaving potentially unknown quantities of encrypted data on CSP systems after their agreement has been terminated is likely to be a violation of their data-retention policy [43].

5.6 Technical Security Considerations

Technical security considerations for cloud environments generally include all those that apply to virtualization technologies, as well as those directly related to the different deployment and service models [43].

5.6.1 Identity and Access Management

Individual user identification and authentication for both CSP and client personnel is essential for access control and accountability. Shared credentials (such as user accounts and passwords) should not be used in the CSP environment—for example, for system administration and maintenance—nor should generic or shared accounts be assigned to or used by clients [43].

The use of a single client credential that covers multiple cloud services for that client is also a potential concern. Client accounts and passwords should be unique for each service, and any account with elevated privilege (such as administrator) should be restricted for a specific service or function, and not used for activities or access that do not require such privilege [43].

5.6.2 Logging and Audit Trails

CSPs should be able to segregate log data applicable for each client and provide it to each respective client for analysis without exposing log data from other clients. Additionally, the ability to maintain an accurate and complete audit trail may require logs from all levels of the infrastructure, requiring involvement from both the CSP and the client [43].

5.7 Proposed Security Framework

The framework aim is to design and develop a security proposal that would be accurate, secure data in shared pool, secure for unexpected intrusions, adaptive and be of real time. The model provides the security of cloud services by the following ways [44]:

5.7.1 Secure Cloud service

The cloud service providers with the highest margins, highest *average revenue per unit* ARPU, lowest operating costs, and lowest churn will have a significant competitive advantage in the long run. To achieve this advantage, they will need a comprehensive cloud service delivery platform and the cost of developing such a platform with security parameter is a factor they will need to take into account. Not all cloud service providers are the same. While some are giants with multiple data centers worldwide, some, in particular niche service providers. That is not all bad computing still is their business, which means they invest all their operating and capital budgets in IT operations. The security of service provider managed by [44]:

- Check out its security staff.
- Ask where its data centers are, how many it has, and what its security parameters and proposals are.
- Separating the company data from company operations has many security advantages.
- Stricter initial registration and validation processes for customers.
- To enhanced credit card fraud monitoring and coordination.
- Comprehensive introspection of customer network traffic.
- Monitoring public blacklists for one‘s own network blocks [44].

5.7.2 Secure Web Platform

Cloud platform services deliver a computing platform and solution stack as a service often consuming cloud applications. It facilitates deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers. The security of the web platform is to securing all content and data traffic - including email, web and identity traffic - moving between an organization and the Cloud [44]. Some schemes that protect the data and its travels within or outside the organization to the Cloud are:

- Analyze the security model of cloud provider interfaces.
- Ensure strong authentication and access controls in concert with encrypted transmission.
- Understand the dependency chain associated with the API. [44].

5.7.3 Secure Cloud Infrastructure

Cloud infrastructure is a platform which holds the development environments and within it one would find managed hosting environment where various applications are built [44]. To secure this Using a secure password management service that protects user ID and password data and can flag users that repeat passwords across various systems. For secure cloud Infrastructure:

- *Lightweight Directory Access Protoco*l LDAP controls and administering credentials that keep access information from being scattered around.
- Running scripts to remove access when employees leave the organization are also proposed for identity management security.
- Determine security breach notification processes.
- Monitor environment for unauthorized changes/activity.
- Promote strong authentication and access control for administrative access and operations.
- Conduct vulnerability scanning and configuration audits [44].

5.7.4 Secure Cloud Data Pool

- *When enterprises adopt cloud computing* and deploy databases in virtual environments, they run the risk of exposing highly-sensitive data to a broad base of internal and external attacks. Here, we enlist strategies to help enterprises protect their data when implementing a database security strategy in cloud or virtualized environments [44].
- *Multi-tenancy*: To be used for single backup system to protect multiple business units or customers and to allocate resources to them dynamically on-demand. Therefore, every storage pool needs to be kept secure and fully independent from the others [44].
- *Chargeback systems*: For data protection resources allocated by end-user needs, storage providers need to track this usage by a wide range of criteria for both chargeback and billing purposes and for infrastructure optimization purposes [44].
- *Robust Reporting*: CC environment need an accurate way to forecast their capacity and processing needs for budgeting purposes. It also needs to analyze usage to optimize available system resources for better efficiencies. Thus detailed reporting and analytics not only helps in managing the current environment but also enables trending and modeling for planning future investments [44].
- *Quality of Service delivery*: Storage pooling enables CC environment to set replication priorities for each pool so that the most mission critical data is replicated before less important data. This QoS orientation can be set to specific backup policies with different retention periods for a particular storage pool [44].
- *Storage Tiering*: Storage tiering is the mechanism to allocate disk drives to a storage pool according to the capacity or performance requirements for a specific set of data under protection [44].
- *Global De-duplication*: De-duplication is a critical part of an effective data protection environment. It is not only necessary for cost-effective optimization of the overall storage capacity but also provides a cost effective WAN

implementation for replication and movement of data to a remote location for disaster recovery [44].

5.8 Some Proposed Techniques

There are solutions to the potential risks associated with cloud computing:

- Data Location Control: Dynamic demotion/promotion of stubs
- Encryption and splitting the data to several places. [45]

Security can also be improved by:

- Using a private cloud, or private area of a hybrid cloud, for client confidential material.
- Using software to automatically encrypt documents at the law firm's end.
- Using security keys that are not known to the provider. [46]

Chapter conclusion

- Cloud service provider CSP, protecting data, and personal/sensitive information, comply with privacy principles that covered the collection, use of information and safe it from disclosure, unauthorized access to achieve a service with a high quality.
- CSP must select specific security requirements depending on the nature of the service and the sensitivity of the data.
- CSP must know what clients want about services type and the required level of security and protection.
- CSP must classify a range of security services, and show it to the clients to determine a suitable service.
- CSP must comply with the classification of clients' data and information to divide the levels of security and protection.
- CSP must be familiar with all vulnerabilities that attacking a services to avoidance it.
- Evaluate the impact of the data protection, and appointing specialist to secure data and reporting the peripherals' about any destruction.

- The Content detection about property rights or intellectual property of data, information or systems is not a cloud provider responsibility; it’s a user responsibility. Also cloud provider irresponsible for other concerns such as child protection, decency: pornography, libel: defamation, prevention of hate speech, and fraud.