**CHAPTER 1:- INTRODUCTION**

**INTRODUCTION OF CLOUD**

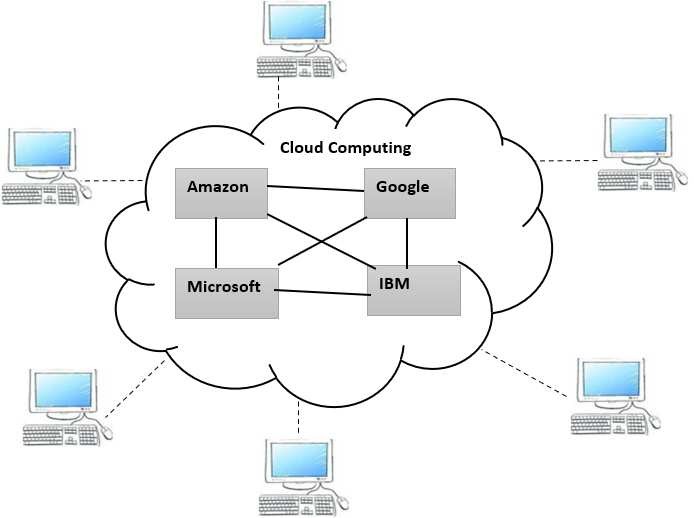
Among different organizations cloud computing has spread widely due to its profits, such as resource pooling, cost reduction, ease of administration and broad network access. By optimizing shared use it enhances the capabilities of physical resources. Outside of regulatory supervision valuable items of the Clients (applications and data) are moved where various clients are grouped together in a distributed environment. On the other hand, security concerns are carriages by this procedure, such as data leakage personally identifiable and theft sensitive information. In cloud computing for decrease the problem of data security several researchers have contributed by renovating a variety of technologies to secure data on cloud, including encryption.

Cloud computing (CC) technology has obtained widespread acceptance due to its proficiency to individuals to make available organizations and enormous resources which can be accessed by the use of the internet anytime and anywhere worldwide [1], [2]. Many information and technology (IT) companies have relocated their businesses to the cloud; a feature-rich cloud experience provided by cloud computing to its users, to shared resources including access, when resources required at lower costs then cloud makes these resources available. These resources may also be released and quickly provided with insignificant administrative effort, and the ability to manage, share, and warehouse data provided by CC, instead of using personal devices or internal resources CC is actually hosted on remote servers [1]. The cloud services can be used by the clients of a number of programs by embracing CC rather than installing the software or buying the software on their own computers [3]. Using a variety of technologies, such as virtualization, web services, operating systems and applications are provided by CC to clients with virtualized resources [1].

**2. ARCHITECTURE OF CLOUD SECURITY**

***2.1. Explaining Cloud Computing***

For describing the web as a location where computing is available as a service and has been preinstalled, then the CC is a metaphor. On the web where data, operating systems, applications, processing capacity and storage all are available among customers and ready to be shared [2]. A collection of data centers referred by CC that offer their services to connect to the internet, and these data centers are founded on the virtualization of their infrastructure [10]. CC is technologically founded on software platform, infrastructure, operating system, database management, cloud app development, system and app management software, network and Internet [2]. CC service providers are companies that provide their customers with CC resources and services in accordance with an individual business model at the request of the customer that are used dynamically. Figure 1 demonstrates the correlation between the most widespread CC service providers, such as Amazon, Google, Microsoft, and IBM.



***Figure 1.1*** *Cloud Computing*

***2.2. Cloud Deployment Model***

CC is categorized into three types [9], [11], [12]: private, public, and hybrid cloud. Private clouds are overseen and managed only for a self-contained organization, and the possessions are not used by other clients, private cloud indicates that from being accessed by unauthorized manipulators, they are protected. The general public and organizations are available by public clouds. Every one of the clients the possessions are shared in between. The possessions they utilize and service provided these are two factors to the clients pay the cloud owner depending on. CSPs administer the physical infrastructure, which is established away from the clients. The mix of the above two types (public and private) are Hybrid clouds [1], [10].

***Figure 1.2*** *Deployment Model*

***2.2.1. Public Cloud:*** In public cloud, where the computing model is hosted the end user has no supremacy over and perceptibility. At the positions of the vendor the cloud retailer hosts the computing model.

***2.2.2. Private Cloud:*** The foremost difference in public cloud and private clouds is that, for a single individual organization it is designed. This cloud computing consist of “reliability” and “scalability” and it is extremely comparable in nature to public cloud.

***2.2.3 Hybrid Cloud:*** This type of cloud deployment model is fundamentally the collaborative venture of the private cloud and public cloud system working together.

***2.2.4 .Community Cloud:*** By various organizations community cloud that is reciprocally consumed and for their extraordinary requirements is commonly framed-up. By the cloud company provider or by the cloud organizations the framework may be functioned and personally -held.

***2.3. Service Models:*** Three key services provided by CC, namely, infrastructure as a service (IaaS), software as a service (SaaS), and platform as a service (PaaS) [1], [9], [11].

***Figure 1.3*** *Service models*

***2.3.1. IAAS (Infrastructure as a service) ≥ Network Architects:***

Infrastructure as a service (IAAS) which consist of storage, networks, processors, memory, and a variety of other resources of computing ,it mentions to CSP hardware infrastructure,. The resources that can be accessed via the internet these are provided as virtualized systems. The crucial resources are under the control of the CSP [1].

***2.3.2. PAAS (Platform as a service) ≥ Application Developers:***

Platform as a service (PAAS) provides through a third-party provider that is platform layer resources who delivers software and hardware tools over the Internet for users and also provides middleware, integrated development environments and operating systems. Only that are shifted over the applications to the cloud, over the underlying cloud infrastructure PAAS does not provide customers control. .

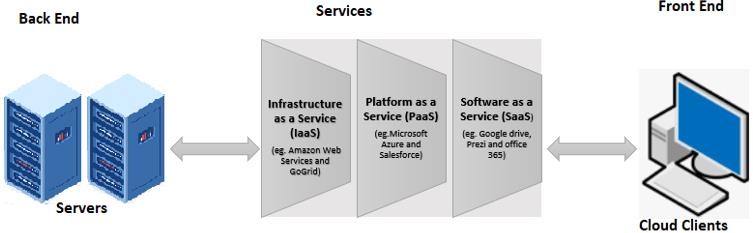
***2.3.3. SAAS (Software as a service) ≥ End Users:***

Software as a service (SAAS) allows consumers over the internet to operate applications as a service. To access it users can simply use the internet instead of install, buy and maintain software. Customers have to pay for utilization rather than possession of the software.



***2.4. CC Service frontend and backend:***

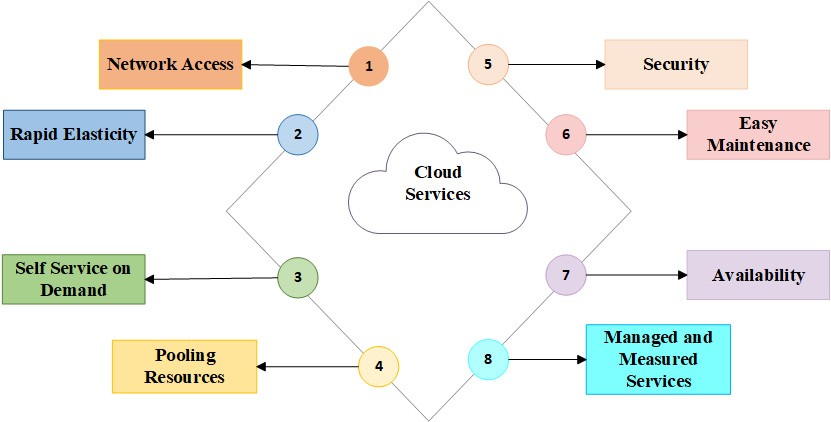
The CC system is segregated into two segments: the back end and the front end. Through a network they communicate with each other, typically over the internet. The cloud clients can see the front end segment. Normally, the customers do not look at the back-end section, which comprises cloud servers, network connection, and their applications. Figure 2 demonstrates the classifications of the architecture of CC and cloud services.



***Figure 1.4*** *CC Service Model*

1. ***Cloud Computing Characteristics :***

Cloud computing assistances organizations safely and enlarge relocation data from physical locations to the ‘cloud’ server, from anywhere at any time that data can be accessed as cloud computing is a promising technology. For the users cloud computing provides a variety of characteristics facilities irrespective of their nature but depend on their effort. Some of the characteristics are as follows[[6](#_bookmark32)]:



***Figure 1.5*** *Cloud Characteristics*

* 1. ***Network Access***

To every user the network is easily accessible, to access users’ data in cloud there will be no inconvenience for the consumers at any machine or any place.

* 1. ***Expeditious Elasticity***

It permits cloud storage to users as per the requirement of every user.CC is Flexible and user friendly in manner.

* 1. ***Self Service on Demand***

Cloud computing provide on demand Self-services as many of them are provided deprived of the agreement of the service provider.

* 1. ***Pooling Resources***

In a unique manner in CC allocation and redistribution of resources are reliant on the requirement of users.

* 1. ***Managed and Measured Services***

Cloud services like security management and the arrangement of data of the cloud storage for every user are controlled by the service providers. Figure [1](#_bookmark1) represents the services mainly provided by cloud computing.

***4. Advantages Of Cloud Computing***

Cloud computing assures many advantages, which are as follows [5], [13]–[15]:

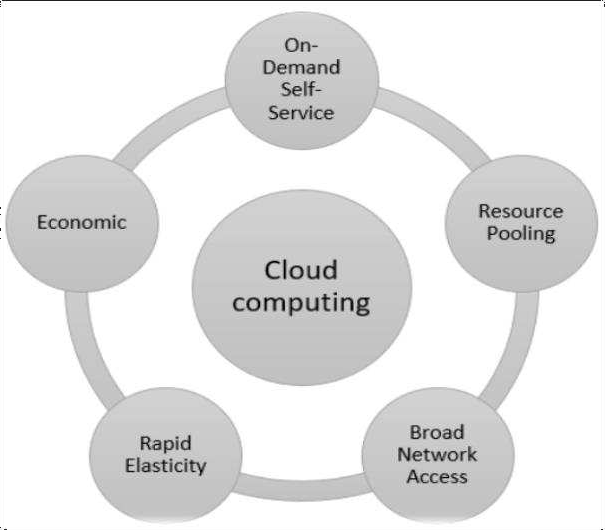
***4.1. On-Demand Self-Service:*** Cloud services (such as network access, network storage, and the server uptime is continuous monitoring) do not require any human being managers. The clients themselves can supervise, provide and manipulate computing resources and IT services as required.

***4.2. Broad network access:*** Over the network from anywhere worldwide a customer can access CC resources with a device and an Internet connection (for instance, computer, smartphone, and PDA).

***4.3. Resource Pooling:*** Among an enormous pool of users a CSP can share CC costs and distribute resources (such as database, servers, storage, networks, applications, and services), permitting users to distribute cloud services according to their requirements and to use data simultaneously connected to the cloud.

***4.4. Rapid elasticity:*** As per requirement services of computing and resources can be scaled up or down quickly and flexibly.

***4.5. Economy:*** For CC users it reduces massive IT expenditures. To maintain and operate the resources the service is paid by the users and used without having to invest in the computing infrastructure necessitated. Additionally, to assigning some services for free there are no additional fees or coverage must be remunerated. Figure 3 demonstrates the advantages of CC.



***Figure 1.6*** *Advantages of CC*

**5. CHALLENGES OF CLOUD COMPUTING:**

Customers of CC services confront a diversity of challenges, which are as follows [16]–[18]:

***5.1. Regulatory Compliance:*** For the integrity and protection of their individual information clients are first and foremost responsible. Even though client data is apprehended by a service provider,.

***5.2. Data Isolation:*** Although encryption is useful in CC, but data is repeatedly shared with those other clients also when using the cloud. It is not a preserve -all.

***5.3. Recovery:*** Even though customers are unaware of the location of their data, in the consequence of a catastrophe a CSP should clarify what will happen to their service and essential data.

***5.4. Location of data:*** Sensitive data are not faithfully where they are accommodated, when CC is utilized. In which their data will be kept the customers are uninformed of the location.

***5.5. Network connection:*** when transferring data between within the data center and hubs of the data there are slow network connectivity causes Internet disruption and performance bottlenecks can lead to giant business losses.

***5.6. I/O operations:***  In a virtual environment do not considerably enhance performance when compared to central processing unit (CPU) time and shared memory. All of the links that make the application execute at the same time required by the immense of high-performance computing applications.

***5.7.*** In a cloud system which has a wide user base, when errors occur, in real time they can only be permanent in the environment of production. Such problems may be difficult to resolving.

***5.8.*** Cloud services must at all times be obtainable. Servers should withstand power outages and distributed denial of service attacks.

***5.9.*** The main challenge of CC is privacy measures of sensitive client data and protecting the confidentiality. It is because they are under the supervision and maintenance of a third party.

***5.10.*** For malicious purposes mistreatment of the cloud services.

***5.11.*** Data preserve and protect from hacking, shortfall, and theft.

The additional issues that required to be concentrated are communication level, network security, storage, big data storage and computational performance, edge computing web app protection, maintenance, reliability, confidentiality, access to data, information integrity, data leakage and authentication .

***I/O operations***

***Figure 1.7*** *Challenges of Cloud Computing*

1. **SECURITY ISSUES IN CLOUD**

To those data centers that are a non-cloud the security of cloud data center is usually indistinguishable [9], [19]. From any threats it is necessary to keeping CC safe. Some security-related and privacy issues that are consideration to be significant for CC are as follows [19]:

* 1. ***Malicious Insiders:*** somebody to the networks who has authorized access and data of an organization and utilize these powers in a fashion that cooperation the confidentiality of the information systems and information of the organization and integrity is called a malicious insider. It is complicated on the organization to identify and has a remarkable effect because most organizations are responsive of this vulnerability.

***Figure 1.8*** *Security Issues in cloud*

***6.2. Account Or Service Hijacking:*** For the reason of software flaws and fraud this threat take place. In this situation, on the cloud to sensitive regions an attacker can gain access, in which he can steal sensitive data and permits.

***6.3. Hypervisor Vulnerabilities:*** the most important piece in virtualization of software is called a hypervisor. The security vulnerabilities have obviously in hypervisors, and often proprietary and remedies are still restricted.

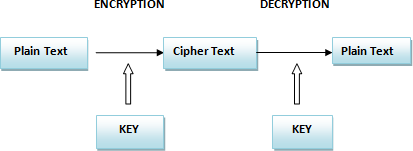
***6.4. Application Programming Interfaces (APIs***) ***And*** ***Insecure Interfaces***: the organizations may face security hazards if an inadequate set of APIs and interfaces are used, security threats such as reuse of passwords, unknown access, clear text authentication or the transmission of content and unacceptable authorizations or nonflexible access management.

***6.5. Cyber-attacks:*** on networks in recent years cyber-attacks and hacking have progressively become a serious threat.

1. **WHY NEED CRYPTOGRAPHY**

In present era for wireless communication the requirement of the internet is getting higher day by day and consequently on insecure wireless channel by users to protection there is necessitate of security such communication. Over the communication channels data sent is susceptible to attacks because of it comprise sensitive information. The hypothesis of Cryptography is emerged to protect the data from external hazard. Cryptography is described as “An art of writing a secret code” [38], Cipher is Methodology to writing such code and which is commonly called Encryption when normal text is converted into cipher text whereas Decryption is known as the opposite perform of encryption where a cipher text is converted into normal text. Cryptography can be classified as modern and classical, the modern cryptography techniques are used for high speed communications and more protected whereas classical cryptography techniques were used to message interception problems and to foil eavesdropping. Modern cryptography techniques are widely used and more protected than the classical ones. Some modern cryptography techniques are such as AES, DES, 3DES, RSA, ECC, ECDH etc.Figure 1.9 represents the terminology of encryption and decryption process**.**

***Figure 1.9*** *terminology encryption/decryption*



**Plain Text:** For the communication purpose the original text is which the user uses is characterized as plain Text. For instance alice sends “how are you” to bob at this time “how are you” is the plain text.

**Cipher Text:** in cryptography the transformation of Plain text into a message (cipher text), out of communication by third party which cannot be interpreted.

For instance: “Hello” is converted into “!@%$#”.

**Encryption:** Encryption is a technique of transforming the plain text into in non-readable form which is called the cipher text.

**Decryption:** Decryption is a technique of transforming the encrypted text reverse into the plain text or normal text.

Cryptography must safeguard four fundamental data protection prerequisites which are as follows: privacy, authentication, non – repudiation and integrity. From [39] we can describe these prerequisites as:

**Privacy -** To make sure that the message can’t be intercepted by third party person.

**Authentication -** In communication where we have to validate the identity of the user involved in this process.

**Non-repudiation**- Here we require to verify the identity of the sender.

**Integrity -** Ensures that original message from sender and received message are indistinguishable that isno modification of data.

**8. Cryptanalyst-** InmodernCryptography Cryptanalyst has proficiency in how to break the cryptographic algorithms and encryption techniques. Now from cryptanalyst it is required to protect our important documents and programs. Over communication network in data transmission security of information means from unauthorized access to keep data protected.

One of many distinguished computing models Cloud computing has been irrespective of the medium and location that provides abundant services, at any location easily accessible, such as networks, unlimited database storage and communications, and others. On the cloud to an ever-increasing reliance it has led to attractive features, leading to raising privacy and a massive volume of data and security concerns. Cloud services significant drawbacks, especially data breaching and data security, could be inaugurated by cloud operators either intentionally or unintentionally. Consequently, to unauthenticated and unauthorized sources limitations on data access should be applied. Since users may be permitted to reuse the data and APIs, source of data breaching can also be devices, causing data loss. Therefore, over the cloud to protect the data cryptographic methods are primarily make use of with the help of different keys by applying encryption/decryption procedures. With the help of keys the two types of techniques that are utilized for the encryption of data are [[1](#_bookmark27)]:

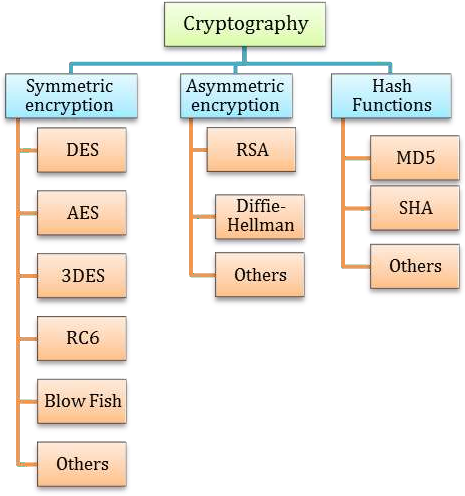
* Asymmetric key encryption of data and
* Symmetric key encryption of data.

public-key cryptography is also known as Asymmetric key encryption. It comprises a couple of keys, i.e., private and public keys for both encryption and decryption of the message, correspondingly. On the other hand, for the security of the data symmetric key encryption is also used, where with the help of a single private key data are encrypted and then decrypted. To encrypt the message the private key is used and to avoid the numerous activity of the hackers. To make sure appropriate protection in embracing the symmetric cryptographic algorithms stalks it has been recognized that the inconvenience from the size of key which requires to be large enough.

**9.Cryptography**

In cloudcomputingtransforming valuable data into incomprehensible format so that no one else can apprehend it apart from the pre-determined consumer is known as encryption and the procedure used are called cryptographic techniques. By using highly efficient mathematical techniques or using code words, through disorganizing words it may be proficient.

From unauthorized access to accomplish the security of information there are many techniques available. For data encryption there are three cryptographic procedures used which are Symmetric, Asymmetric and Hashing procedures.



***Figure 1.10*** *Cryptographic techniques*

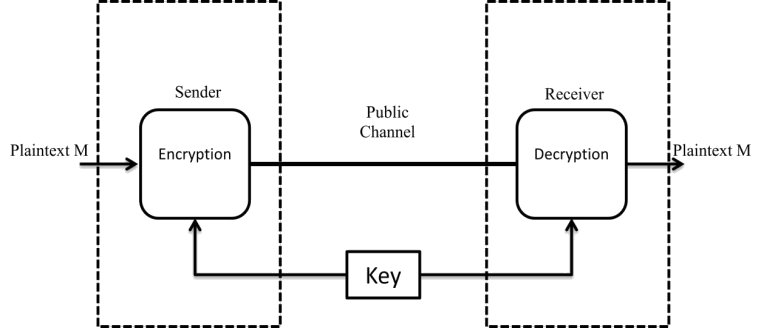
***9.1. Symmetric Or Private Key Cryptography –***Symmetric key Cryptography is a branch of cryptography in which the both encryption and decryption algorithms are executed with a solitary key. On such schemes to perform brute force attacks it is away from the scope of existing computational resources, given key segments of randomness and sufficient size. On the other hand, on a single key due to the extreme dependence, in the communication of the key cryptography schemes lies from the sender to the receiver securely a major factor towards implementing symmetric.

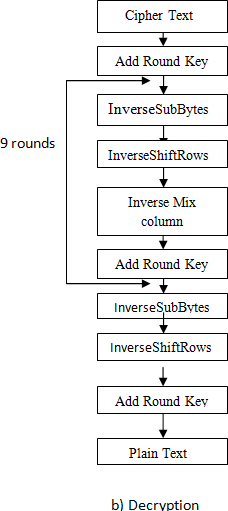
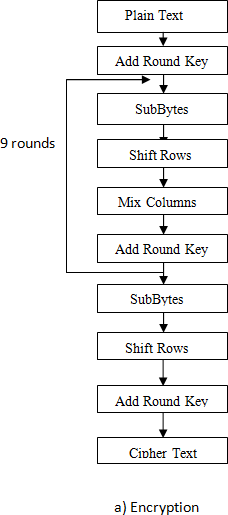
Figure1: Symmetric key Encryption

***9.1.1. AES* :** AES stands for advanced encryption standard. A normalized form of Rijndael algorithm is AES. It is six times faster than triple DES and it was developed by Belgian Cryptographers.In contrast to DES, AES is originated on the conception of permutation and substitution. Fiestel Network does not used by AES (Fiestel Network is used for the production of block ciphers and it is a symmetric structure).AES works on a mechanism of 4x4 matrix bytes to encrypt or depending on the size of the key exhausted.

NIST (National Institute of Standards and Technology) declared AES as a Centralized Information Processing Standard in the year 2001. Due to its high security, efficiency, and simplicity AES is a repeatedly used encryption technique. Because it uses the identical key for both encryption and decryption processes so AES is known as a symmetric block cipher. Three block ciphers AES-192, AES-128, AES-256 are used by AES. Depending on the block size the Encryption process comprises several rounds, with 10 rounds for a 128-bit key, 12 rounds for a 192-bit key, and 14 rounds for a 256-bit key.Using AES for encrypting data below are few steps comprised in this process. AES algorithm involves of 4 stages each and every round of the encrypting data.

***Figure 1.11*** *Steps of AES algorithm*

* ***i.i)****.* ***SubByte****:* This is the first stage of AES and in this stage given by a predefined relation of each byte is substituted with a value. Using predetermined S-boxes containing of 256 values these substitutions are carried out.



* ***ShiftRows***: This is the second stage of AES in this stage, in the NIST standard by guidelines recognized the elements accomplished from the S-boxes are then shifted right, or on a need-by-need basis selected independently.
* ***MixColumns***: This is the third stage of AES in this stage where each column is mix then as a polynomial it delivered and then by an encoding polynomial multiplied. In the Galois Field to give a polynomial then the result is distributed by an irreducible polynomial.
* ***AddRoundKey****:* This is the last stage of AES in this phase by a simple key a round key generated to the state array schedule is added.

Over a Galois extension field all calculations are done (28). With the similar number of rounds the Decryption Algorithm is the identical algorithm, in converse direction. In the message to recurrent sequences of characters vulnerabilities is pertaining, improper key selection have been discovered and verified to be exploitable. in spite of this the computation time do not reduce by these attacks to make it feasible for brute force searches prerequisite by enough an amount. AES can be reflected ‘secure’ as it bounded by current computational resources. Across many security protocols wired and wireless the most extensively accepted symmetric key cipher is AES.

***9.1.2*. DES** The Data Encryption Standard is a broadly used cryptographic algorithm in a pre-quantum world that has to brute force searches already been proven to be vulnerable. In spite of this, this vulnerability may be overcome by enhancing the complexity of the key, leading to the use of enhanced schemes such as the Triple-DES (3DES), with 2 or 3 keys which may be utilized, in a comprehensive search the number of operations required exponentially augmenting.

On a Feistel-Round structure DES is founded, where the message is fragmented into two halves, in each round which go through alternate operations [6]. Being processed per round each message block is 64 bits leading to 32 bits. For each round the first 32 bits are XOR’ed with the consequence of a Feistel Function in this round which the remaining 32 bits takes as input. In the same way, in the subsequent round, with the processed bits the unchanged bits are swapped, and the round is again carried out. DES algorithm comprises of 16 such rounds, by an Initial Permutation (IP) it started off and with a Final Permutation (FP) it ended up that is the opposite of the IP.

Given below is the Feistel Function :

* **Expansion**: To the instigating and terminate of the existing 4-bit block, by appending and duplicating the last and first bits of the subsequent and preceding 4-bit block the 32-bit input is transformed to 48-bits.
* **Key Mixing**: through a simple key schedule that is obtained from the original key in each round corresponds to a subkey of 48-bit. The output is XOR’ed with the subkey of the Expansion stage.
* **Substitution**: In this phase, we split the output that we get from the key mixing stage so the consequence split into 8-bit to 6-bit blocks, through non-linear S-box transformations which are passed, by an NIST standard the S-boxes have been predetermined and it can be utilized as a lookup table. Each S-box takes 6-bits as input and it will output 4-bits, so it may be overtaken onto the subsequent round as the consequent output is thus transformed back to 32-bits.
* **Permutation**: As a final point, in a P-box the outputs of S-box are reorganized in a manner that safeguards in the subsequent round that across 4 different S-boxes the result of each S-box is distributed. Through the S-boxes and P-boxes DES can be responsible for appropriate diffusion and confusion to make sure the output stay on random enough so a brute force search would be the solitary way to break the cipher. DES is not recommended for use because it has already been confirmed to be broken.

DES was first broken by the DESCHALL Project in 1997. In the present day, DES has been considered as vulnerable to attack, and in computational power with the increasing growth each year, to being virtually unfeasible as a cipher the prerequisite time has been decreased. On or after 2017, with the utilization of Rainbow Tables it was observed that the speediest DES break (for selected-plaintext attack), they attaining the key in less than 25 seconds.

To prevail over the effortlessness of breaking DES an effort was created through getting higher effective key length to proliferation computation trials required. Through the 3DES Algorithm this overcome has been put into operation.

***9.1.3. 3DES:*** To the vulnerability of DES Triple DES be responsible for a solution by using 3 different standalone keys K1, K2, K3 due to its small (56-bit key size) and by ‘expanding’ the size of key each of 56-bits. An Encryption- Decryption-Encryption sequence is carried out by Encryption of the simple text. Using DES the plaintext is first encrypted with the use of key K1. Then using the DES intermediate text is decrypted with the use of key K2. As a final point using DES the consequence is encrypted with key K3, by which the ciphertext is given [6]. The time complexity can be increased of Brute Force, by using 3 different values of K1, K2, K3 founded on how we select the keys. With an effective key length of 168-bits the maximum security we can achieve of 3DES has to offer. However, due to the small block size the probability for collisions is increases as this attempt was also shown to be vulnerable. By the sweet32 attack this was exploited [7] wherein in 236∗2 trials collisions can be found.



E

Cipher

**t**ext

**K1**

K2

Plain text

D

E

K1



K1

Plain text

D

E

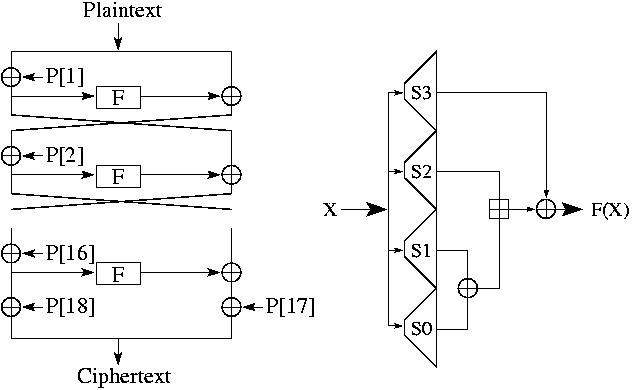
K2

Cipher

text

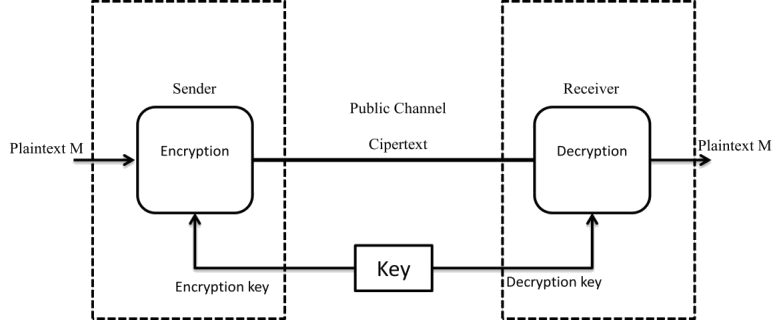
K1

D

***9.1.4. Belowfish:*** In belowfish with a block size of 64 bits from 32 bitsto 448 bits with length of the adjusting key sizes belowfish also a symmetric cipher constructed as an alternative way for more profitable DES and AES. It’s a 16-round cipher. On this encryption most conceivable recognize attacks are birthday attacks and for files of size in excess of 4 GB should not be used. Commercially, it can be used as alternative to AES and it is efficient cipher in encryption process.

***9.1.5.RC4***: It isalso called Rivest Cipher four as RC4 is manufactured by Bokkos Rivest. for confidential constituting of the plain content in this the stream figure is exploited. On the off chance to operated mackintosh efficiently and effectively the basic square figures don’t come into sight, on the off chance doable is bit-fluttering assault and furthermore they’re not legitimately authorized as the stream figure assault is additionally powerless.

**9.2. Asymmetric of public key cryptography:** to encryption and decryption of the message uses two different keys in Asymmetric key (also known as public key encryption). The public key can be used to encrypt messages and is made publicly available. To decrypt received messages the private key can be used and is kept secret. Such as RSA, ECC, Diffie-Hellman etc. are asymmetric key encryption algorithm. Primarily, to encrypt a message use a key (public key). Secondly, to decrypt a message another (private key) is used.

***Figure2***: *Asymmetric key Encryption*

**9.2.1.RSA:** RSAincorporates variable key size and block size encryption as it is a technique of public cryptosystem. The crucial steps that involved in RSA are: Two dissimilar prime numbers are generated, Evaluate t As product of two, Now calculate phi(t), Discover d such that d \* e = 1, Private key is (1, d) and Public Key is (1, e). It is the most deceptive shortcoming is that in case two numbers should be of correspondent size and are of enormous length then it takes additional time. The below text elaborated a brief introduction of the standard algorithms

**9.2.2.ECC**

Based on elliptic curve theory the Elliptical curve cryptography (ECC) is a technique of public key encryption that can be operated to generate smaller, quicker, and more efficient cryptographic keys. ECC has more complex and difficulty to retrieving the plain text and in breaking the key so this is a significant feature that is the key strength.

In the form ECC efficient types of cloud services are make available which is utilized for the data encryption and data decryption. Asymmetric encryption and decryption of data are used by these services. It assistances the RSA for encryption and decryption process of data so it is more efficient than others; to the symmetric encryption and decryption of data the size of the key is shorter paralleled. For instance, if for the key the size of the data is 1020 bits, by using the RSA scheme in ECC it will be decreased to 163 bits. Furthermore, using smartphones for network access ECC is more appropriate. To breach the personal information of the user or to blackmail them breach some data many hackers are in a urgency. That is why for users ECC is specifically made, the consumers who are accessing their crucial data with slightest safeguarded devices that can be effortlessly hacked [[8](#_bookmark34)].

**9.2.3.Diffie-Hellman**

Asymmetric Cryptography means simply Public-Key Cryptography to encrypt and decrypt the message which utilizes private and public keys. To exchange the secret key this conception was applied by Diffie and Hellman for receiving and sending the messages. In cryptography one of the most analytical problems between two communicating devices is exchanging the key. It was not about launching a shared-secret key, but it was about to accomplish it in such a manner that communication between the devices any person who is there at the devices do not obtain out the key. The first creditor of Diffie- Hellman algorithm was Ralph Merkle and this algorithm is entitled after Whitfield Diffie and Martin Hellman. Over a public channel this algorithm bring about the key exchange secure [37].

Mathematics uses the Diffie-Hellman algorithm that is using the communication channel discrete logarithm and modular arithmetic for making a shared key for both sender and receiver where sender and receiver select a common prime number p and q as it’s primitive root, where q<p[37].

**9.3. Hashing:** There are different cryptographic hashing algorithms used for message authentication some are like MD2, MD4, MD5, MD6, SHA-1, SHA-224, SHA-256, SHA-512, Whirlpool etc.

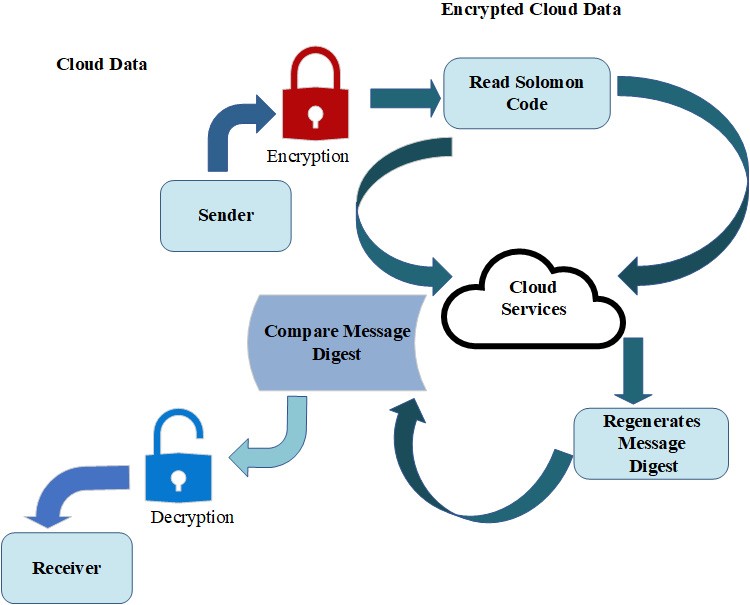
**9.3.1. Message Digest**

**9.3.2. SHA256**

***10. Cryptographic Cloud Services***

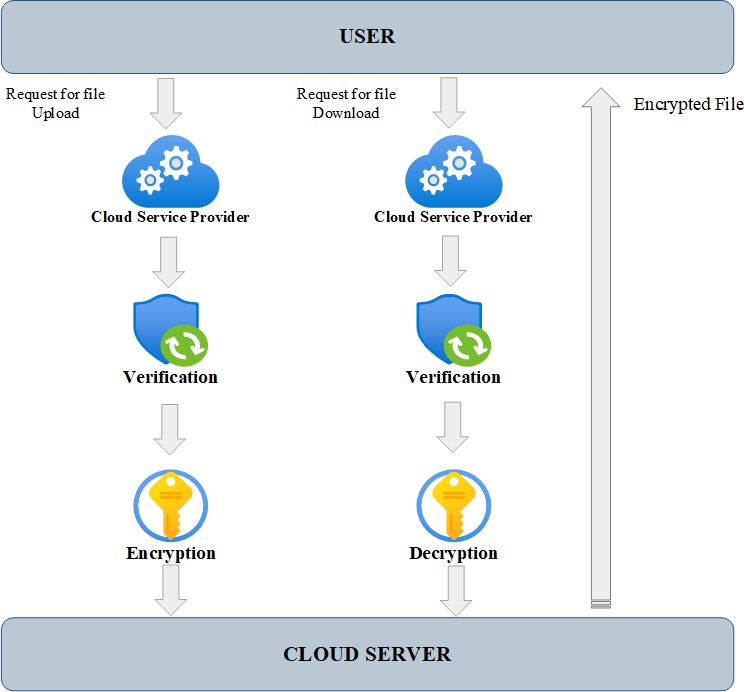
To obtain the encryption and decryption of data to the users in cloud storage current augmentations have make available different services done deprived of the participation of a third party in a proficient manner. This improves the protection of the system for enhancing the system in addition to the effectiveness of the storage for quick retrieval and reliable accessibility of information. Through this service by different types of customers the distribution of cloud resources can be done without any difficulty and by safeguarding more storage improve the potential of the system subsequently the implementation of the cryptographic techniques [[7](#_bookmark33)].

Figure [2](#_bookmark2) shows that the cloud storage services have the different forms. At the cloud server it can be perceived that the data between receiver and sender are being stored along with encrypted and decrypted. Over the cloud storage it also stand for the confident transmission of data.



**Figure 2.** Cloud storage services.

1. ***Cloud Storage Server:*** Figure [3](#_bookmark3) demonstrates that on cloud server the information and consumer stored; the figure illustrates that at the server how the data are being accessed confidently and the procedure of how a consumer demand of data has been processed and.



**Figure 3.** Cloud storage server.