

**A NOVEL METHOD FOR MAINTAINING SECURITY  
ON CLOUD COMPUTING**

A Dissertation submitted in partial fulfillment of the requirement for the

Award of degree of

**MASTER OF TECHNOLOGY**

**IN**

**INFORMATION SYSTEMS**

Submitted By

**SATYA DEO KUMAR RAM**

(2K13/ISY/24)

Under the esteemed guidance of

**Dr. N. S. RAGHAVA**

Associate Professor



**Department of Computer Science & Engineering**

**Delhi Technological University**

**Bawana Road, Delhi-110042**

**2012-2014**

i

## CERTIFICATE

This is to certify that the thesis entitled “A Novel Method for Maintaining Security on Cloud Computing” submitted by Satya Deo Kumar Ram(2K13/ISY/24) to the Delhi Technological University, Delhi for the award of the degree of Master of Technology is a bona-fide record of research work carried out by her under my supervision. The contents of this thesis, in full or in parts, have not been submitted to any other Institute or University for the award of any degree or diploma.

Place: DTU, Delhi

Dr. N.S Raghava

Date: \_\_\_\_\_

Associate Professor

Department of Computer Science & Engineering  
Delhi Technological University, Delhi

## **ACKNOWLEDGEMEN**

First I would like to express my gratitude towards my supervisor Dr. N. S. Raghava, Associate Professor, Department of Information Technology for his able guidance, support and motivation throughout the time. It would not have been possible without the kind support and help of many individuals and Delhi Technological University. I would like to extend my sincere thanks to all of them. I would like to express my gratitude and thanks to Dr. O.P Verma (Head of Dept.) for giving me such an opportunity to work on the project. I would like to express my gratitude towards my parents & staff of Delhi Technological University for their kind co-operation and encouragement which helped me in completion of this project. My thanks and appreciations also go to my friends and colleagues in developing the project and people who have willingly helped me out with their abilities.

**Satya Deo Kumar Ram**

Roll No.: 2K12/ISY/08

Dept. of Information Technology

Delhi Technological University

## ABSTRACT

The emergence of cloud computing in recent years has brought an interest from different organizations, institutions and users to take advantage of its services and applications. Because of providing a very attractive package of services, cloud technology has collected a huge attention from academia, IT industry and government organizations. Cloud computing promises scalability and on-demand availability of resources. Day-by-day number of users on the internet goes on increasing; and attacker are also on same path it becomes very necessary to provide efficient security mechanism over cloud computing to ensure the security to the millions of user requests on it. Security problem can be at any level. Therefore, one of the important issues which need a major consideration of the researchers is strong security in cloud computing systems. A number of cryptography algorithms are proposed by various researchers, to solve this problem. Two kinds of cryptography algorithms are there one is symmetric and other is asymmetric. Since users lose their control after storing of information at cloud storage. So there is need of strong security mechanism so that even cloud service provider must not be aware of user's data. Many symmetric and Asymmetric algorithm is proposed but many of them has broken by attacker or is about to be broken. There is a new encryption technology has proposed, that is DNA symmetric algorithm which is computationally very less expensive than existing cryptography algorithm because no complex mathematical algebra is involved but cipher is very complex than other one. The basic idea behind this encryption technique is the exploitation of DNA cryptographic strength, such as its storing capabilities and parallelism in order to enforce other conventional cryptographic algorithms. In this study, a binary form of data, such as plaintext messages is transformed into sequences of DNA nucleotides. Some algorithm is already there such as OTP DNA symmetric algorithm. But it has problem because of OTP has same size as that of plaintext. Proposed methodology is more reliable and more powerful than the OTP DNA symmetric algorithms. This method takes three symmetric key which don't depend on text message size. It is simple to execute but provides strong security because of it generating strong cipher containing DNA four bases combination.

# TABLE OF CONTENTS

<b>TITLE</b>	<b>PAGE NO.</b>
CERTIFICATE .....	(ii)
ACKNOWLEDGEMENT.....	(iii)
ABSTRACT .....	(iv)
LIST OF FIGURES .....	(xi)
SCREEN SHOTS... ..	(xii)
LIST OF TABLES .....	(xiii)
<b>CHAPTER 1: INTRODUCTION</b>	
1.1 RESEARCH BACKGROUND.....	12
1.2 CHALLENGES AND MOTIVATION.....	13
1.3 OBJECTIVES AND CONTRIBUTIONS.....	14
<b>CHAPTER 2: CLOUD COMPUTING</b>	
2.1 INTRODUCTION.....	15
2.1.1 CLOUD COMPUTING DEFINITON.....	18
2.1.2 CLOUD COMPUTING.....	19
2.1.2.1 CLIENTS.....	20
2.1.2.2 DATA CENTERS.....	21
2.1.2.3 DISTRIBUTED SERVERS.....	21
2.2 CLOUD EVOLUTION.....	21
2.2.1 BRIEF HISTORY.....	22
2.2.2 COMPARISION WITH RELATED TECHNOLOGY.....	23

2.2.2.1	UTILITY COMPUTING.....	24
2.2.2.3	AUTONOMIC COMPUTING.....	25
2.2.2.4	GRID COMPUTING.....	26
2.3	CLOUD COMPUTING ARCHITECTURE.....	27
2.4	CLOUD SERVICE MODEL.....	27
2.4.1	SOFTWARE AS SERVICES.....	28
2.4.2	PLATFORM AS SERVICE.....	28
2.4.3	INFRASTRUCTURE AS A SERVICE.....	29
2.4.4	OTHER SERVICES.....	29
2.5	CLOUD DEPLOYMENT MODEL.....	29
2.5.1	PRIVATE CLOUD.....	30
2.5.1.1	ON - PREMISE PRIVATE CLOUD.....	31
2.5.1.2	EXTERNALLY HOSTED PRIVATE CLOUD.....	32
2.5.2	PUBLIC CLOUD.....	33
2.5.3	HYBRID CLOUD.....	33
2.5.4	COMMUNITY CLOUD.....	34
2.6	CLOUD CHARACTERISTICS.....	34
2.6.1	TECHNICAL CHARACTERISTICS.....	34
2.6.1.1	VIRTULIZATION.....	35
2.6.1.2	MULTI TENANCY.....	35
2.6.1.3	SECURITY.....	35
2.6.1.4	PROGRAMMING ENVIRONMENT.....	36
2.6.2	QUALITATIVE CHRACTERISTICS.....	36

2.6.2.1	ELASTICITY.....	36
2.6.2.2	AVAILABILITY.....	36
2.6.2.3	RELIABILITY.....	37
2.6.2.4	AGILITY.....	37
2.6.3	ECONOMIC CHARACTERISTICS.....	38
2.6.3.1	PAY- AS- YOU- GO.....	38
2.6.3.2	OPERATIONAL EXPENDITURE.....	38
2.6.3.3	ENERGY EFFICIENCY.....	38
2.7	VIRTULIZATION AND CLOUD COMPUTING.....	38
2.7.1	KEY CHARACTERISTICS OF VIRTULIZATION.....	38
2.7.1.1	MANAGED EXECUTION.....	40
2.7.1.3	PORTABILITY.....	40
2.7.2	VIRTUALIZATION TECHNIQUES.....	41
2.7.2.1	FULL VIRTUALIZATION.....	41
2.7.2.2	PARA VIRTUALIZATION.....	41
2.8	ISSUES IN CLOUD COMPUTING.....	42
2.8.1	SECURITY.....	42
2.8.2	PRIVACY.....	42
2.8.3	AVAILABILITY.....	43
2.8.4	INTEGRITY.....	43
2.8.5	RELIABILITY.....	43
2.8.6	LEGAL ISSUES.....	44
2.8.7	VENDOR LOCK-IN.....	44

2.8.8	COMPLIANCE.....	44
-------	-----------------	----

### **CHAPTER 3: OVERVIEW OF CRYPTOGRAPHY AND NETWORK SECURITY**

3.1	SECURITY GOALS.....	44
3.1.1	CONFIDENTIALITY.....	45
3.1.2	INTEGRITY.....	45
3.1.3	AVAILABILITY.....	46
3.2	ATTACKS.....	47
3.2.1	INSIDE ATTACKS.....	47
3.2.2	OUTSIDE ATTACKS.....	47
3.3	THREAT OF CONFIDENTIALITY.....	47
3.3.1	SNOOPING.....	48
3.3.2	TRAFFIC ANALYSIS.....	48
3.4	ATTACK THREATENING TO INTEGRITY.....	48
3.4.1	MODIFICATION.....	49
3.4.2	MOSQUERADING.....	49
3.4.3	REPLAYING.....	49
3.4.4	REPUDIATION.....	49
3.5	ATTACKS THREATENING AVAILABILITY.....	53
3.5.1	DENIAL OF SERVICES.....	53
3.6	OTHER CATEGORY OF ATTACKS.....	53
3.7	SECURITY SERVICES AND MECHANISM.....	53
3.7.1	SECURITY SERVICES.....	53



3.7.1.1	DATA CONFIDENTIALITY.....	53
3.7.1.2	DATA INTEGRITY.....	54
3.7.1.3	AUTHENTICATION.....	54
3.7.1.4	NON REPUDIATION.....	54
3.7.1.5	ACCESS CONTROL.....	55
3.7.2	SECURITY MECHNISM.....	55
3.7.2.1	ENCIPHERMENT.....	55
3.7.2.2	DATA INTEGRITY.....	56
3.7.2.3	DIGITAL SIGNATURE.....	56
3.7.2.4	AUTHENTICATION EXCHANGE.....	56
3.7.2.5	TRAFFIC PADDING.....	56
3.7.2.6	ROUTING PROTOCOLS.....	56
3.7.2.7	NORMALIZATION.....	57
3.7.2.8	ACCESS CONTROL.....	58
3.7.2.9	RELATIONSHIP WITH SERVICE AND MECHANISM.....	58
3.8	CRYPTOGRAPHY.....	58
3.8.1	SYMMETRIC KEY ENCIPHERMENT.....	59
3.8.1.1	TRADITIONAL SYMMETRIC KEY CIPHER.....	59
3.8.1.1.1	SUBSTITUTION CIPHER.....	59
3.8.1.1.2	MONOALPHABATIC SUBSTITUTION CIPHER.....	61
3.8.1.1.3	POLYALPHABATIC SUBSTITUTION CIPHER.....	61
3.8.1.1.4	SHIFT CIPHER (CEASER CIPHER).....	61
3.8.1.1.5	TRANSPOSITION CIPHER.....	62

3.8.1.1.5.1	COLUMNAR TRANSPOSE.....	62
3.8.1.1.5.2	DOUBLE TRANSPOSITION.....	64
3.8.1.1.5.3	MYSZKOWSKS TRANSPOSITION.....	64
3.8.1.1.5.4	DISRUPTED TRANSPOSITION.....	64
3.8.2	SIMPLE MODERN CIPHER.....	65
3.8.2.1	XOR CIPHER.....	66
3.8.2.2	ROTATION CIPHER.....	70
3.8.2.3	SUBSTITUTION CIPHER: S-BOX.....	72
3.8.2.4	TRANSPOSITION CIPHER: P-BOX.....	72
3.8.2.5	STRAIGHT P-BOX PERMUTATION.....	72
3.8.2.6	EXPANSION P-BOX PERMUTATION.....	72
3.8.2.7	MODERN ROUND CIPHER.....	72
3.8.2.8	TRIPLE DES.....	72
3.8.2.9	AES (ADVANCE ENCRYPTION STANDARDS).....	72
3.8.2.10	IDEA.....	73
3.8.2.11	BLOWFISH.....	73
3.8.2.12	CAST-128 (CARLISLE ADAMS AND STANTFORD TRAVARES).....	74
3.8.2.13	RC5.....	74
3.8.2.14	ECB (ELECTRONIC CODE BLOCK).....	75
3.8.2.15	CBC (CIPHER BLOCK CHAINING).....	76
3.8.2.16	CIPHER FEEDBACK.....	78
3.8.2.17	OUTPUT FEEDBACK.....	78
3.8.3	ASYMMETRIC KEY CRYPTOGRAPHY.....	79

3.8.3.1 RSA.....80

3.8.3.2 DIFFIE HELLMAN..... 80

**CHAPTER 4**

4 PROPOSED METHODOLOGY..... 81

4.1 INTRODUCTION.....81

4.2 PROPOSED ALGORITHM (NEW DNA CRYPTOGRAPHIC TECHNIQUE).....82

4.3 OUTPUT OF ENCRYPTION TECHNIQUES..... 85

**CHAPTER 5**

CONCLUSION AND FUTURE WORK.....

**CHAPTER 6**

6 REFERENCES.....

# CHAPTER 1

# Introduction

## 1.1 RESEARCH BACKGROUND

Cloud computing has made a very significant improvement over earlier computing technologies in terms of services they offer. Previously, users use Grid computing and Distributed computing which are not able to provide much flexibility as that of provided by Cloud computing. There are number of attractive features are available in cloud computing systems that made it popular these days. Cloud computing follows pay-as-you-go model and enables on-demand provisioning of computing resources in an elastic manner. This standard has made cloud computing system more demanding in the area of business applications where huge amount of cost is required to setup infrastructure. With the invention of cloud technology users can easily rent the infrastructure, runtime environments and services. Also different users may utilize the benefits of cloud computing in many domains according to their needs. Cloud service provider is the main entity, enabling various users to make use of different cloud services according to their choice. Cloud service providers offer their customers the illusion of unlimited computing resources, network, and storage capacity often coupled with a 'frictionless' registration process where anyone with a credit card can register and start using cloud services. Some cloud service providers even offer free limited trial for some periods. In Cloud Computing one of the major tasks of the cloud service provider is to assign service to their user. Requests to several nodes present in the cloud. This assignment of tasks among the node in cloud should be very efficient as possible as. For an efficient cloud system, the total effort and the processing time for the entire cloud user request should be as low as possible, while being able to manage the various affecting constraints such as heterogeneity and high network delays. These days Cloud computing has become so popular in the area of Information and Communication Technology (ICT), therefore the requirement of large and powerful data centers comes into picture. Due to rapid increase in the number of cloud users, cloud providers also have to boost the capabilities of

different cloud components, it can be done by increasing their number, increasing their power or both. This kind of situation may result into a very huge network comprising cloud users, datacenters, nodes, virtual machines and user tasks.

## **1.2 CHALLENGES AND MOTIVATION:**

With emergence of cloud technology which is at boot in market of storage and computational task at lower cost. At any component there can be security problem such client side, at transmission channel, at server side etc. Almost cloud is able to deploy any infrastructure of company for which company has to pay. At every layer cloud is able to provide services to their customer at software or application types service, at development level of service like it can provide the tool for developing software or any application. Infrastructure such as hardware, network and specific server system but it is bitter true there is major security at every layer. Since business organization or any customer will think once before storing their own cloud because of sensitive data. More sensitive information is kept by business organization which can be their rich information for business logic processing or an important decision is taken by that organization based on their repository information. Cloud service provider must have satisfactory level security solution to make faith that data stored by cloud user is secure. There can be security issue in virtualization of cloud's component. Like an attacker can inject their harmful code into database of cloud or inject kernel code into OS virtualization and can take control of all virtual machines which are used by cloud providers. Since users lose their control from data. So there is need of such technique which should not be dependent even on cloud administrator. Since on same virtual environment many virtual machines are provided to cloud user, maybe this data can be scattered to other VM.

### 1.3 OBJECTIVES AND CONTRIBUTIONS:

This thesis studies security related issues in cloud computing. The primary objective of this thesis is to provide an efficient security mechanism, which helps in making strong relationship between cloud service provider and users. In cloud computing environment security can be ensured by using effective security mechanism on user's virtual machine and then provisioning of virtual machine to different nodes in the system. The major contributions are as follows: A more efficient technique for security in cloud computing is introduced. The technique's center of attention was on prevention of the any kind of attacks. This attack can be at virtualization level such as OS level virtualization, application level virtualization, server level virtualization and network virtualization, at kernel level also.

A comparative analysis of security algorithms in cloud computing systems. Many factors like geographical distribution of nodes, peak hour usage of services over different locations, scalability, response time, and different threats are analyzed in depth for each of these algorithms.

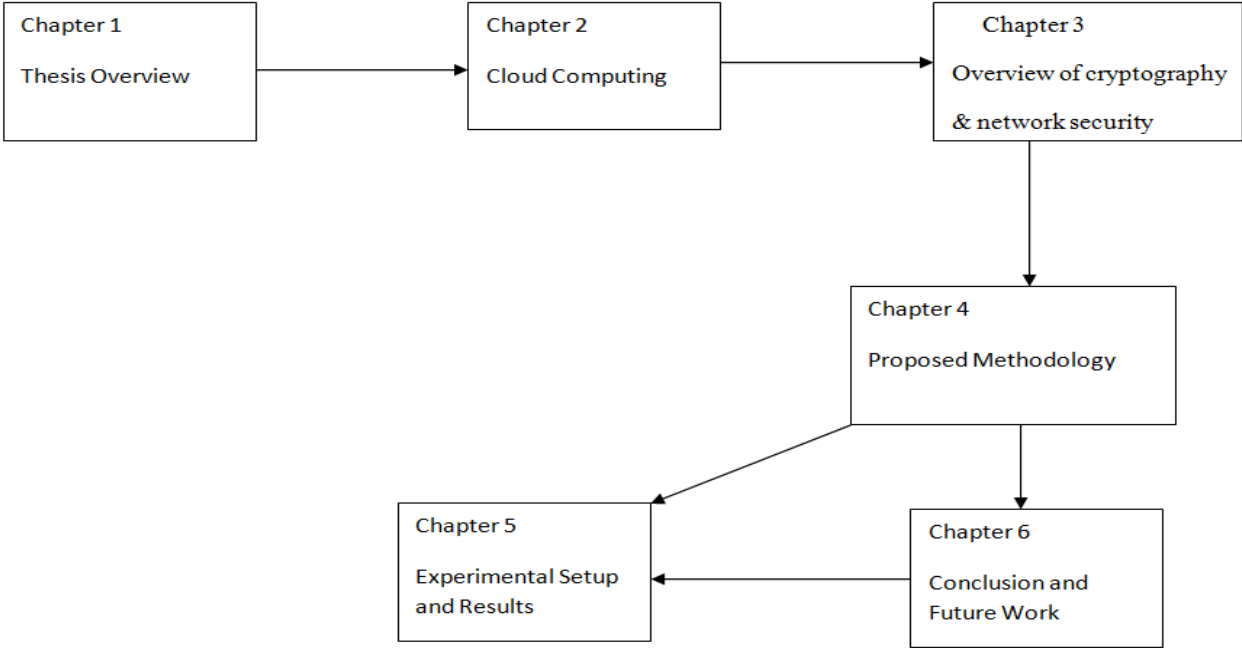


Figure 1.1

## CHAPTER 2: CLOUD COMPUTING

### 2.1 INTRODUCTION

In previous decades have given the idea of information processing, in a more efficient manner. With the emergence of cloud computing headache of storing, processing and accessing the data through internet at larger scale disappeared now. The network based computing idea led to the evolution of Grid computing in early 1990s and since 2005, to utility computing which ultimately brought to the development of cloud computing. From very long time researchers are trying to give utilities as services to its user. User can demand for software, platform and hardware resources from a provider through internet and charged on the usage basis. So cloud computing is a path to utility computing by IT giants like Microsoft, IBM, Hp, Amazon, Google etc. Within very short span of time this technology has spread over the globe.

#### 2.1.1 CLOUD COMPUTING DEFINATION

Since 2007, term cloud has got more popularity in IT industry. There are vast number of definition are given by the various researchers. Everyone has defined it according to different- different application. But there is no standard and common definition for cloud computing. Some of definition has chosen among all definition for cloud computing in this paper that as follows.

*NIST: "Cloud computing is a model to enable ubiquitous, convenient on demand network access to a pool of shared resource that is network, server, storage and application. These can be rapidly provisioned and released with minimum management effort or service provider interaction"*

## A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:

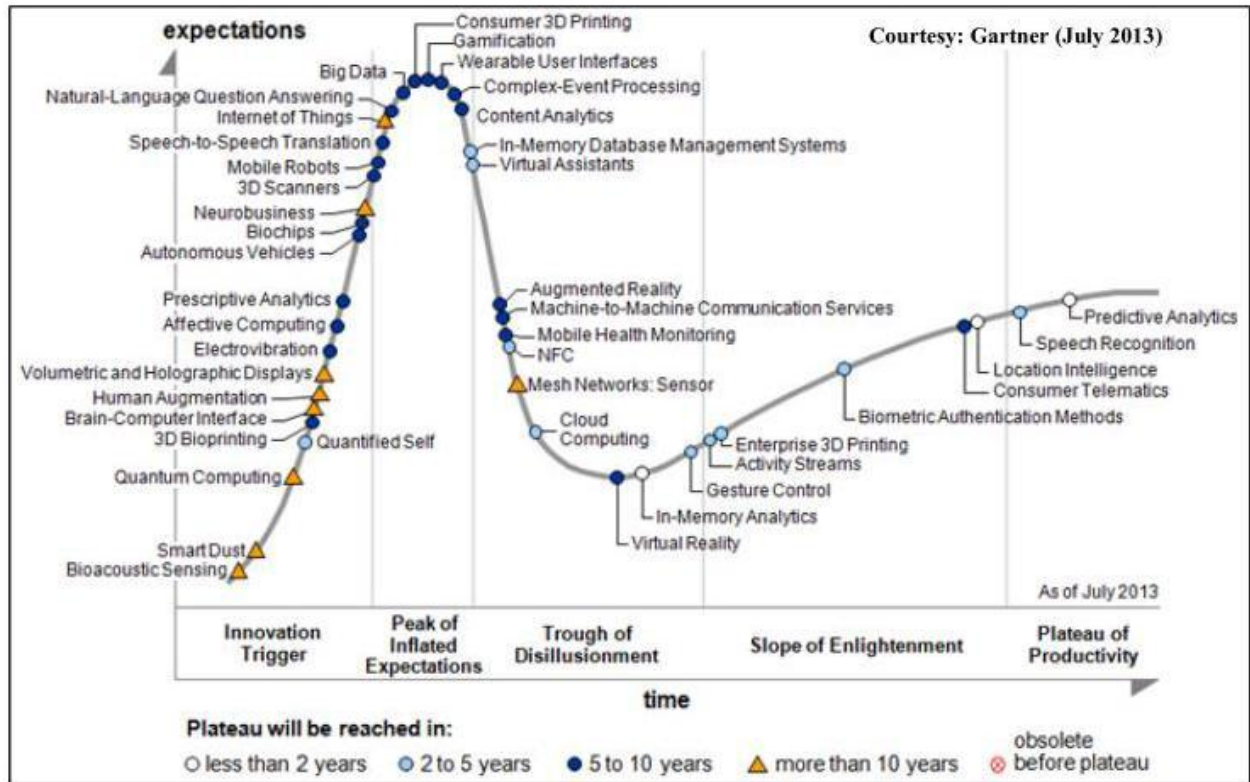


Figure 1.2 Cycle for Cloud Computing

- *FOSTER: A large -scale of distributed paradigm that is driven by the economics of scale ,in that a pool of abstracted virtualized, dynamically-scalable, managed storage, computing power ,platforms and services are delivered on demand too intersected external customer over internet.*
- *FOSTER: A large -scale of distributed paradigm that is driven by the economics of scale ,in that a pool of abstracted virtualized, dynamically-scalable, managed storage, computing power ,platforms and services are delivered on demand too intersected external customer over internet.*



U.S. National Institute of Standards and Technology provide a specific and goal oriented definition of cloud computing. It also specifies the characteristics of cloud computing with its delivery and deployment models. But Foster definition has a little bit differences in the context of educational representative, have focused on various methodological features that differentiate the cloud computing from other distributed computing paradigm. Computing entities are virtualized and delivered as services are example of it. These services are dynamically driven by economics –scale.

A term “Clouconomics” has given by Joe Weinman which defines cloud computing economical perspective, which is discussed below:

1. **C**ommon Infrastructure: it is a common and standard resource pool that is made available to all the cloud users.
2. **L**ocation Independence: user can access its resources or services from anywhere around the globe. That leads the better performance and gives better response of system in time.
3. **O**nline connectivity: There is need of maintain consistent connection via internet to access the services or resource over the cloud.
4. **U**tility Pricing: pay-per-use pricing and benefits the as per their demand.
5. **O**n-Demand Resources: Scalable elastic resources are provisioned and de-provisioned without delay or costs associated with change.

## 2.1.2 CLOUD COMPUTING

Some elements from topological aspect of cloud are clients or users, the data center and distributed servers. This component combines the cloud as single unit. This component can be shown by this figure.

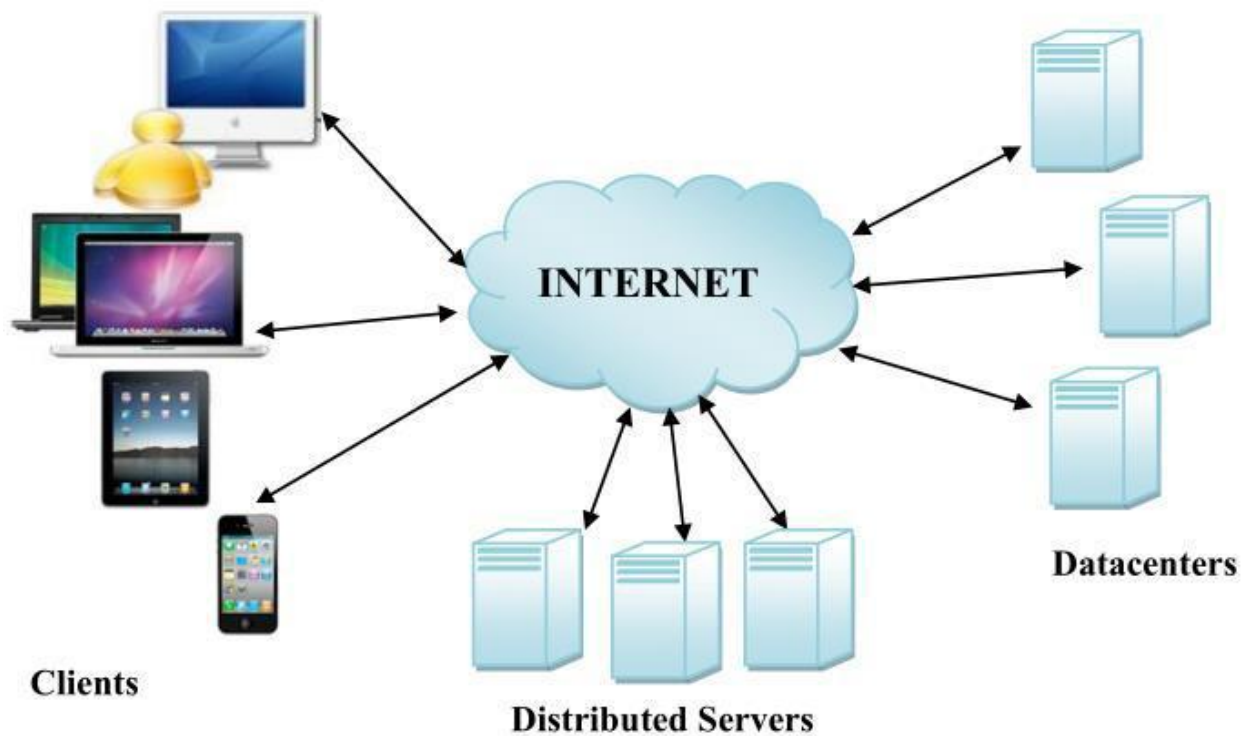


Figure.2.2: Components of Cloud

Each of the components has specific role to deliver services on demand of cloud users. All this components communicates over the entire network according to the requirements and configuration.

Role of the these component is defined below

### **2.1.2.1 CLIENTS**

Clients are computer which are used in our day to day works but it may be a PDA, a laptop, a mobile phone or a tablet computer. But all these clients should able to access the cloud computing resources or say cloud computing interface through internet. With help of these device end users are able to access the cloud computing interface through internet and can use the services or application as per user choice.

### **2.1.2.2 DATACENTERS:**

It is one of the core elements of cloud computing system. It consists of various nodes occupying a large room. These datacenter are configured by the CSP. Configuration is based on various factors such as cloud computing service model deployment model.

### **2.1.2.3 DISTRIBUTED SERVERS:**

The servers, also called nodes, need not be deployed at the same location; it may be distributed geographically as per convenience of cloud service providers. From user point of views these server seems to be work together, without knowledge of actual location of servers. Distributed server increases the fault tolerance of network.

## **2.2 CLOUD EVOLUTION:**

The stream of providing cloud computing services on rent by investing on large distributive facilities is not new. It can be seen from previous decades, that similar kind of technology are used in IT industry with regular modification. Birth for this sort of technology has given by mainframe technology in 1950. From there time technology has evolved and been refined. A steps of favorable condition leads the realization cloud computing.

## 2.2.1 BRIEF HISTORY

This complete collection is allocated to the demanded end user, is called virtual this environment is provided by the help of hypervisor environment. Means with the help of hypervisor say VMware to execute multiple operating systems simultaneously in an separated environment. Virtualization is one of the most important key in cloud computing. In 1990s, telecom companies are started to offer Cloud computing is started to emerge from 1950s, when mainframe technology become popular. Mainframe technology allow to multiple users to access a central computer through their separate channels. This terminal is responsible for providing access facility to the mainframe. After this evolution, in 1970s, Virtual machine was introduced. One of the most famous hypervisor that is VMware is used for the virtualization. First of all this virtualization technology provides the virtual machine concept in cloud computing. On hypervisor cloud provider install different software and operating and provide a separate chunk of hardisk, chunk of memory and one OS the VPN (virtualizes private network) network which offer cheaper and better qualities services.

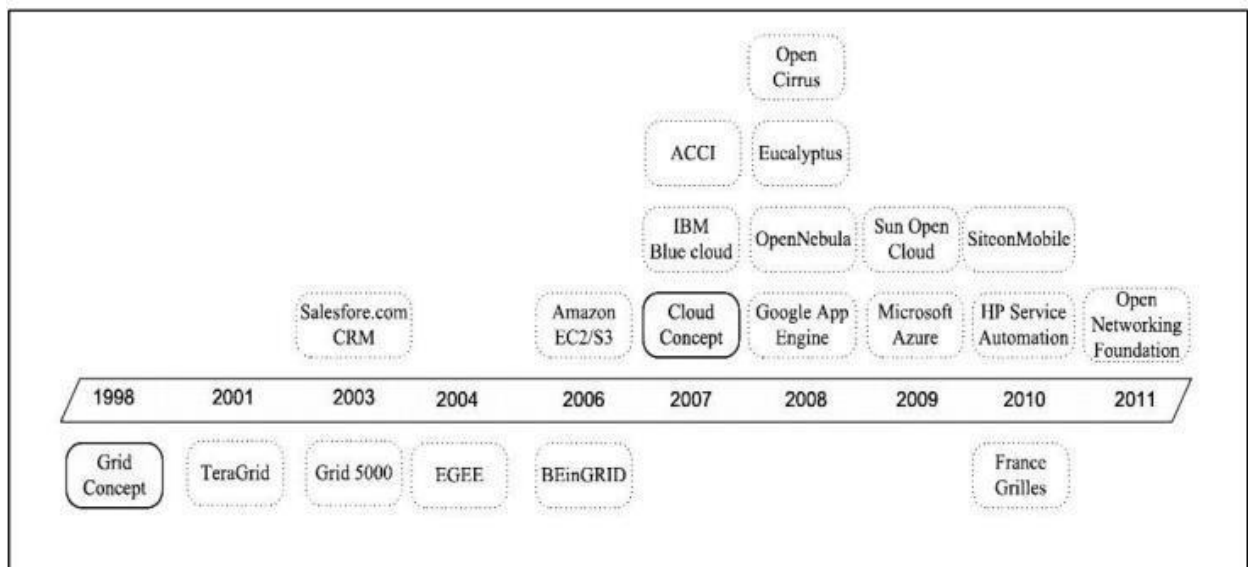


Figure.2.3: Emergence of various related technologies during different years

This series continued with the introduction of cluster computing after the grid computing. These all together bring the cloud computing. In above figure there can be shown cloud the emergence of cloud computing.

### **2.2.2 COMPARISION WITH RELATED TECHNOLOGY**

Cloud computing consists of services oriented architecture, autonomic computing, virtualization, utility computing and grid computing. The cloud computing system sometimes it confused with related technology like utility computing, grid computing and autonomies computing.

#### **2.2.2.1 UTILITY COMPUTING**

It is one the very old technology that came into picture from 1960s. John McCarthy gave a speech at MIT in 1960s about utility computing. In this computing user can access the service based on their requirement without worrying about whether the service is hosted. But utility computing is good choice for demanding application which is needed less resource. It does not required the cloud computing and can run on any server environment.

User may consume same way as they used other utilities like power, gas and water.

#### **2.2.2.2 AUTONOMIC COMPUTING**

This computing first of all purposed by IBM in 2001. It performs the task according to some adoptive policies. Autonomic computing contain adoptive policies is used for self-management of computing system. It had brought several fields of computing with motive of creating self-managed.

### **2.2.2.2 AUTONOMIC COMPUTING**

This computing first of all purposed by IBM in 2001.It performs the task according to some adoptive policies. Autonomic computing contain adoptive policies is used for self-management of computing system. It had brought several fields of computing with motive of creating self-managed.

### **2.2.2.3 GRID COMPUTING**

Grid computing came into picture in mid 90s.Grid computing is the collection of computing resources, storage resources and many network resources to achieve a common and large goal. Means if an application needs large amount of resources which is not available at a single location but available at multiplication then there is need of some technology so that it connects all required resources to accomplish the application. User can access the large

## **2.3 CLOUD COMPUTING ARCHITECTURE**

Cloud computing support any IT services that can be used as utility and delivered through internet. Cloud computing provides facility to clients to deploy their application on cloud without worrying about computing power, storage and location. It is possible for business clients or organization to request cloud services at any level, may be at application services level, and may at infrastructure level and development platforms. It is possible to organize all these characteristics of cloud computing system into layered view covering the entire stack from hardware appliance to software system.

Layered architecture of cloud can be seen as following

Computational power with unlimited storage capacity by using the grid computing. Grid computing is just like a commuter network topology in which each computer resources are shared with every other computer in at system. These resources are like processor power, memory and data storage. It is just like collection of similar computer which are running on the same operating system.

## A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:

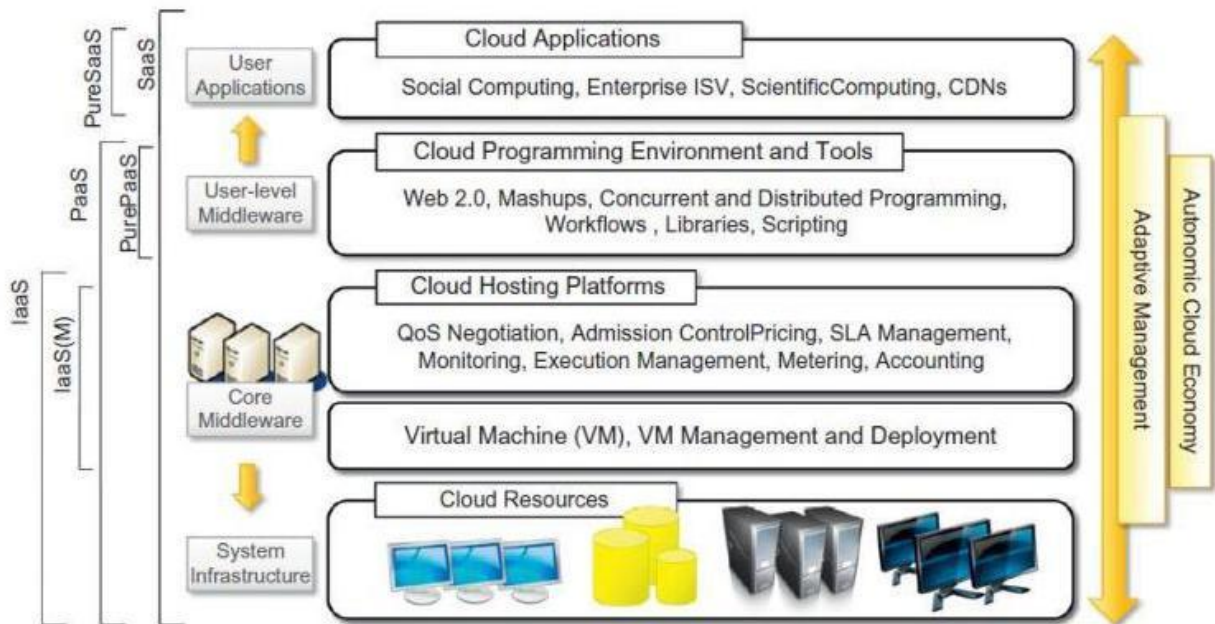


Figure.2.4: Cloud Computing Architecture

## 2.4 CLOUD SERVICE MODEL

Once a cloud is deployed by clients and is ready to use by its consumer. It has to be decided that how to use this services offered by cloud. Three way through which cloud services can be delivered, software, platform and infrastructure. These are the three services model which is used by the cloud service provider. It can be studied as below.

### **A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:**

Software as services (SaaS) is software deliver model. In Traditional software application there was need to purchase it and install it onto user's computer. But in this model user have not purchased and install software onto user's system which is need of their application. Consumers have not worried about infrastructure and development platform .Consumers has not worried about required hardware, network administrator, developer, programmer to deploy their application. So consumers have only to use software that they need to run their application. User is nothing to worrying about maintenance and configuration of software and hardware. It is responsibility of third party whom they are registered with. It is associated with pay as you go subscription model .Application can be accessed through internet such as web based services. User can make use of cloud services by registering on cloud services provider site. It specially designs to facility many concurrent users at a time.

There are many reasons; SaaS are beneficial to clients and personal.

- **There are no additional hardware costs:** Processing power is required to run the user application is provided by the cloud providers.
- **There is no initial set up costs:** once the user subscribes application is ready to use.
- **Pay-per-usage:** If user is required to use a piece of software for a fix amount of



time then user will be charged only for that period and user are free to be halted at any time.

- **Usage is scalable:**

User's demand is scalable at any time. User can demand for more storage and computational power at any time.

- **Updates are being automatic:**

- **Can be access from any location**

Since SaaS services are accessed through Web browser so there is need of web security, Extendable Markup Language (XML) encryption, secure socket layer etc.

Some famous SaaS service provider companies such as Facebook, Google docs, NetSuite, Microsoft online.

## **2.4.2 PLATFORM AS SERVICE**

Platform –as-a –service (PaaS) is collection of software and development tools which are hosted on the cloud provider's server. It provides the environment and developing tool that allow to developers to build their applications. It provides tools to user to create their own application. It is mid-layer of service mode. It is integrated set of developer environment can come to build their application. It brings developer to complete software development life cycle maintenance. Mainly in this service model developer build the application that is provide to the cloud service user. It provides the facility to user to develop their own application using programming language, libraries, services and tools. In SaaS users have full of control over the deployed application and their hosted configuration.

Some features provide by the cloud provides as a tools to users.

### **Operating system**

- ✓ Database management system
- ✓ Server software
- ✓ Storage
- ✓ Network
- ✓ Tools for design and development
- ✓ Host Sever side subscription environment

Some popular PaaS service provider companies are window Azure, Engine Yard and Google Aap Engine.

### **2.4.3 INFRASTRUCTURE AS A SERVICE (IaaS)**

Infrastructure –as-a service, resources are shared with contracted clients as pay –per-use fee. It minimizes the huge investment in computing hardware like processing power, networking device, and servers. Main theme it provides only hardware required by user to develop their to own application. Means here clients have not worried about infrastructure as a basics network device, processing power and hardware to develop the application. So in IaaS, clients have own developer, networker administrator which only responsible for configuration of network. A user can deploy and can run any operating system like Linux, Solaris and other software like Mat lab, code block, eclipse, Net beans etc. User is free from hurdle of managing the cloud infrastructure which was required to run their application. But has to manage the storage, operating system and deployed the applications. Mean user only service provided by the service provider is infrastructure like hardware, storage now it is client responsibility to manage own development, network storage etc.

Some Companies that provides IaaS services such as Amazon, Go grid, and 3 tera

Some popular PaaS service provider companies are window Azure, Engine Yard and Google Aap Engine.

### **2.4.3 INFRASTRUCTURE AS A SERVICE (IaaS)**

Infrastructure –as-a service, resources are shared with contracted clients as pay –per-use fee. It minimizes the huge investment in computing hardware like processing power, networking device, and servers. Main theme it provides only hardware required by user to develop their to own application. Means here clients have not worried about infrastructure as a basics network device, processing power and hardware to develop the application. So in IaaS, clients have own developer, networker administrator which only responsible for configuration of network. A user can deploy and can run any operating system like Linux, Solaris and other software like Mat lab, code block, eclipse, Net beans etc. User is free from hurdle of managing the cloud infrastructure which was required to run their application. But has to manage the storage, operating system and deployed the applications. Mean user only service provided by the service provider is infrastructure like hardware, storage now it is client responsibility to manage own development, deployment, network storage etc.

Some Companies that provides IaaS services such as Amazon, Go grid, and 3 tera

### **2.3.4 OTHER SERVICES:**

Some other services such as security as services, testing as services are domain specific service.

Figure 2.5 service models in cloud computing.

## A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:

---

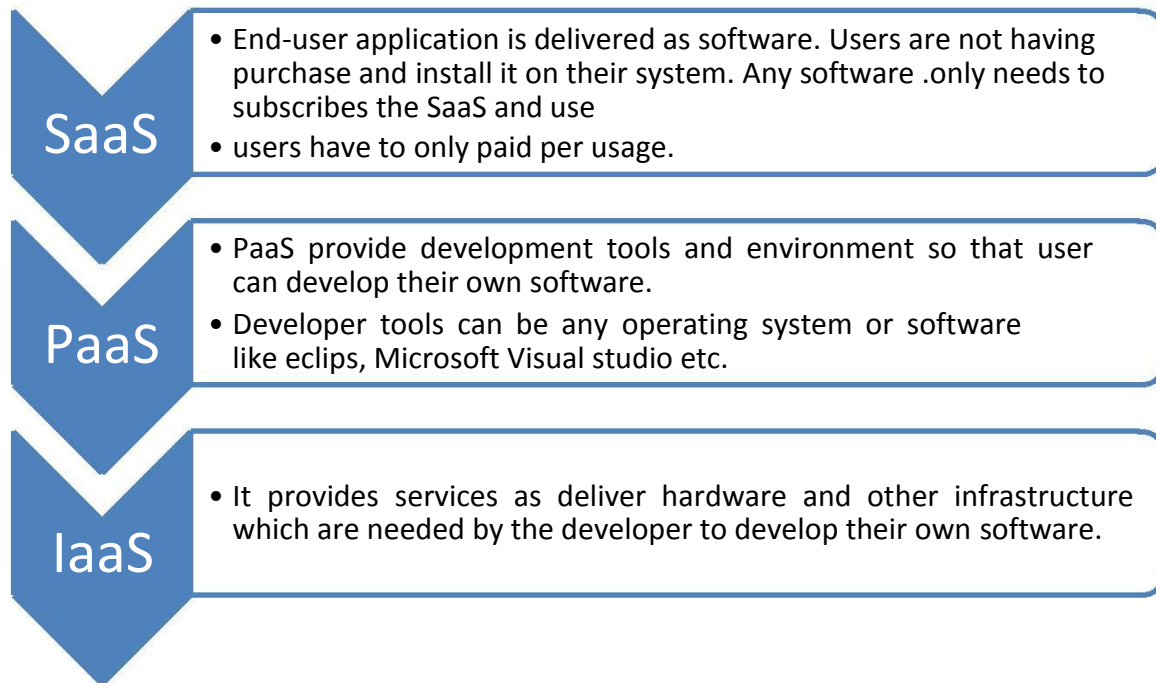


Figure 2.4

### 2.5 CLOUD DEPLOYMENT MODEL:

There are numbers of cloud users who wants cloud service of different size such as infrastructure of different size and each one of the infrastructure needs different kinds of management and also different user groups wants different size of infrastructure based on services listed by cloud. It defines the services and its boundary.

These deployments are as follow

#### 2.5.1PRIVATE CLOUD:

Private cloud computing is particularly involves a secure cloud environment in which only the specified clients can operate. Private cloud is accessible by only a single organization with own control and privacy. In private cloud services model, draws their services from a district computer system but it may be hosted internally or externally or may be accessed across private line or through encrypted connection by public networks. An organization can request to third party to create its own private cloud infrastructure. Some big organization such as Google, Microsoft has their cloud infrastructure which supposed to be more secure than public cloud. An organization having private cloud can serve its user its own cloud like Google providing services such as Gmail, Drive, GoogleApp-engin and many more. On the basis of deployment of cloud, private clouds are divided into two parts

### **2.5.1.1 ON-PREMISE PRIVATE CLOUD:**

It is also known as internal hosting private cloud computing. This private cloud hosted privately within its own datacenter. Benefits are to standardize the process and better privacy can be achieved. But disadvantage is, size and scalability can restricts the person to choose this kind of Model.

### **2.5.1.2 EXTERNALLY HOSTED PRIVATE CLOUD:**

This cloud hosted externally with cloud provider. It provides special cloud environment with full privacy. This type of cloud only needs for those who do not want to share their physical resources to the public cloud.

Hcloudstart and eBay is two popular providers of private cloud deployments.

The features and benefits of private clouds are:

- ✓ **Higher security and privacy:**
- ✓ **Costs and energy efficiency:**
- ✓ **Improved reliability:**

### **2.5.2 PUBLIC CLOUD:**

These types of cloud services are provided in a virtualized environment and built using pool of shared physical resources and accessible over a public network like internet. Services are provided to multiple clients using same infrastructure. Means there services publically available. The cloud which are managed and operated by a government, academic Institution or business organization. There are some companies which provide public cloud

such as EC2, Google's AppEngine, Sun cloud, IBM's Blue Cloud and Windows Azure Services Platform.

### 2.5.3 HYBRID CLOUD:

Hybrid cloud integrate, services provided by both private and public computing.

An organization may have both type of operation sensitive and non-sensitive. So in private cloud, non-sensitive operation may use the public cloud services. This will maximize the efficiency of organization.

Hybrid cloud can be implemented as follow.

- Portioned cloud providers team to provide both public and private services as integrated services.
- Individual cloud provider may offer complete package of hybrid cloud services.
- The cloud provider who managed private cloud of an organization should themselves sign up to public cloud and then integrated this into their infrastructure. Infrastructure of these clouds is totally different. It may be combination of private, public or community cloud.

An enterprise can implement hybrid cloud, hosting to host its e-commerce site within a private cloud so it is secure and scalable but their broacher in a public cloud with more cost effective.

Hybrid cloud can offer feature to their user:

#### **Scalability:**

An IaaS offering, could follow the hybrid cloud and provide a financial business with storage for clients within a private cloud, then allow association on project planning documents in the public cloud – from there they can be accessed by multiple users from any location.

#### **Security:**

#### **Flexibility**

### 2.5.4 COMMUNITY CLOUD:

This cloud is similar to concept of grid computing and also multitenant platform which allow many of companies work on same platform; with this they have similar needs and concern. There are some specific communities of users from different business organizations.

Consider a private firm in which there are two main business domains which works separately from one another. In that cases a firm can create two community clouds for the separate working of the two domains. The security requirements and the other policies for the two domains are totally different. It is multi-tenant infrastructure which is shared among

various organizations from a specific group with common computing requirement.

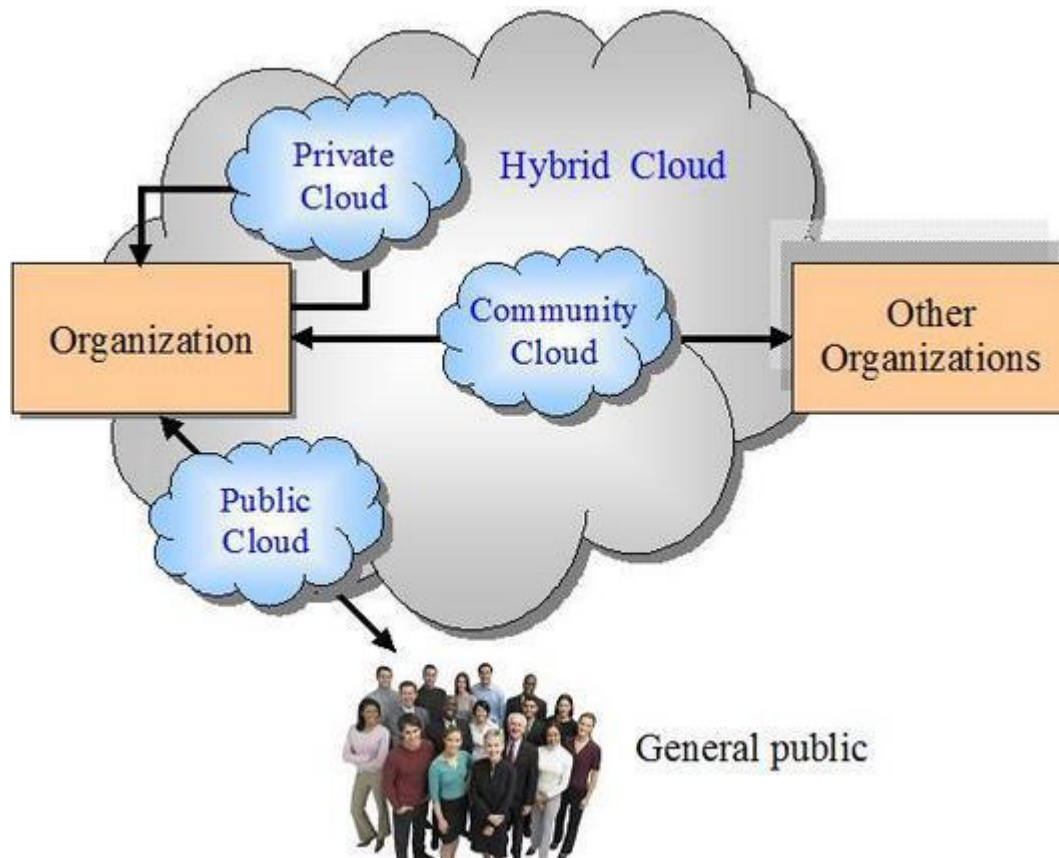


Figure 2.5.4

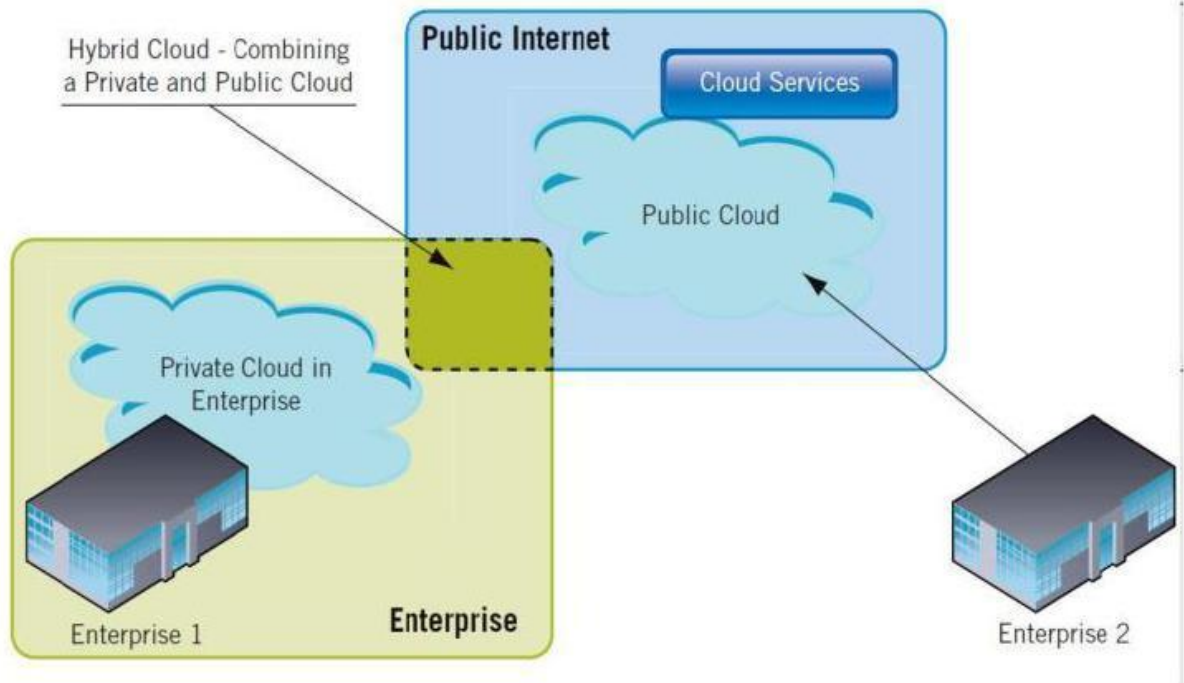


Figure.2.6: Private, Public and Hybrid Cloud Deployment

### 2.6 CLOUD CHARACTERISTICS:

Cloud computing is expressed by the aspects of several existing technologies. These Technologies could be, utility computing, service oriented architectures, grid computing, autonomic computing or internet of things. This's why it was sometime said that cloud computing is nothing but the identical previous concept with new label.

Some characteristics of cloud computing:

- ✓ **On-demand self-service:** service is provided to user's demand without interaction with cloud provider. Cloud provider can add and delete the users and can change storage network and software as needed.
- ✓ **Broad network access:** user can access their services using smartphones, tablets, laptops and office computer.



✓ **Resource pooling:**

The cloud allows your employees to enter and use data within the business management software which is hosted in the cloud at the same time, from any physical location, and at any time.

✓ **Rapid elasticity:**

Cloud computing system can quickly and easily can add or remove users, software features, and other resources which are available. Cloud can be flexible and scalable to suit user's immediate business needs.

✓ **Measured service:** Due to affordable nature of the cloud, users have to only pay for what they use.

### 2.6.1 TECHNICAL CHARACTERISTICS:

Technical characteristics serve the basis for functional and economical requirements. Generally a technology is not completely unique, but is encouraged from its predecessor technologies.

#### 2.6.1.1 VIRTUALIZATION:

It is one of most important characteristics of cloud .It must be called backbone of cloud

Computing without it existence of cloud has no much importance. Virtualization is only things that make possible to provide virtual machine to the users to do their computational task on cloud. Using hypervisor such as VMware is used for virtualization. On VMware they software such as operating system corresponding to some chunk of memory and some chunk of hard disk, on this there become possible to make as many possible chunk of memory and hard-disk and installation of software or operating system to make a virtual machine that seems to user as he is provided with a separated and unique virtual machine. Virtualization can be at many components such as virtualization on operating system, virtualization of servers, application level virtualization etc.

In cloud computing virtualization enables:

1. System security, as services can be isolated running on the same hardware.
2. Performance and reliability, as application migration is possible from one platform to another.
3. The development and administration of services offered by a provider.
4. Performance isolation.

### **2.6.1.2 MULTI-TENANCY:**

It is also mandatory thing in cloud computing. Multi-tenancy allow to multiple user to make use of resources concurrently. User are separately charge based on their usage .For example in real life such as there are multi storey-building .the owner of building provides the housing facility to all tenant and tenant pay him accordingly.

### **2.6.1.3 SECURITY:**

Security is one of most essential factor in cloud to make belief in cloud by user.

Users have both types of data sensitive and non-sensitive data which needs proper security inn any system. In every service level agreement the terms and conditions of cloud services provider is mentioned which provide security and trust of users.

### **2.6.1.4 PROGRAMMING ENVIRONMENT:**

Programming environment should be such as, it is able to extract all required features of cloud computing like C#.Net can be used with Window Azure tool in Microsoft visual Studio. Microsoft Visual studio 2012 onwards, Window Azure Tool can be integrated

Through tool option in Visual studio. It should be able to address the issues like multiple administrative domains, resource heterogeneity, cloud federation, exception handling in highly dynamic environments, etc.

### **2.6.2 QUALITATIVE CHARACTERISTICS:**

It explains properties or qualities related to cloud computing. Every cloud service

Providers have different provision of these qualitative characteristic to their users.

#### **2.6.2.1 ELASTICITY:**

Cloud computing makes user free from problem related with expansion of any resources .user can request for sudden expansion or any required length of resources can be requested. Elasticity is one attractive features in cloud computing.

#### **2.6.2.2 AVAILABILITY:**

It is capability of cloud computing that make sure to their users; service is guaranteed anytime anywhere through dedicated internet connection. Availability mean services must be available at any time.

#### **2.6.2.3 RELIABILITY:**

Cloud service provider makes ensure to their users there will be no loss of services or user's data. That means services and data lost due to any reason can be recoverable because of huge storage capacity of cloud and duplicity of data at different server and location.

### **2.6.2.4 AGILITY:**

It is basic requirement of cloud computing. This feature of cloud ensure that cloud provider is capable and will be capable of providing quick response with or without any kind of changing in resources or length or number of resources on-line. Users are not need of wait for business hours to get their network. They can connect from, bank, platform, home or from anywhere. Virtual machine may be moved automatically and instantly to other servers. Storage and other resources can be dynamically allocated as that of requirement to satisfy user needs without any intervention.

### **2.6.3 ECONOMIC CHARACTERSTICS:**

From economical perspective one should focus on the cloud market trends. This is one of best feature of cloud which make more valuable than other computing technology. Economically it is cheaper than any computing in market. That's why it has higher demand in computing market.

#### **2.6.3.1 PAY-AS-YOU-GO:**

User has to pay only for services which are used by them. Whatever resource is used by cloud user will be charged at reasonable cost. In early time a lot of infrastructure cost is required for establishing own business.

#### **2.6.3.2 OPEARTINAL EXPENDITURE:**

It is highly reducible in cloud computing. Users can enter into the real world of cloud easily, by having a credit card also some cloud service providers offer limited free subscription. They can rent the infrastructure for sporadic intensive computing tasks.

## A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:

### 2.6.3.3 ENERGY EFFICIENCY:

It is high in demand now a day in every domain. IT domain is moving towards highly efficient technology. Many surveys show that in upcoming time most of the cost will be spent on reducing power consumes. Cloud provider is look for reducing power consumption of listed resources delivered as services to the users.

### 2.7 VIRTUALIZATION AND CLOUD COMPUTING:

Virtualization is one of the basic components of cloud computing. In IaaS it plays very important role. Sometimes is called hardware virtualization. Virtualization abstracts the basic resources and simplifies their use, isolates users from one another, and supports replication which, in turn, increases the elasticity of the system. Virtualization came early than cloud computing but cloud gets more popularity than virtualization.

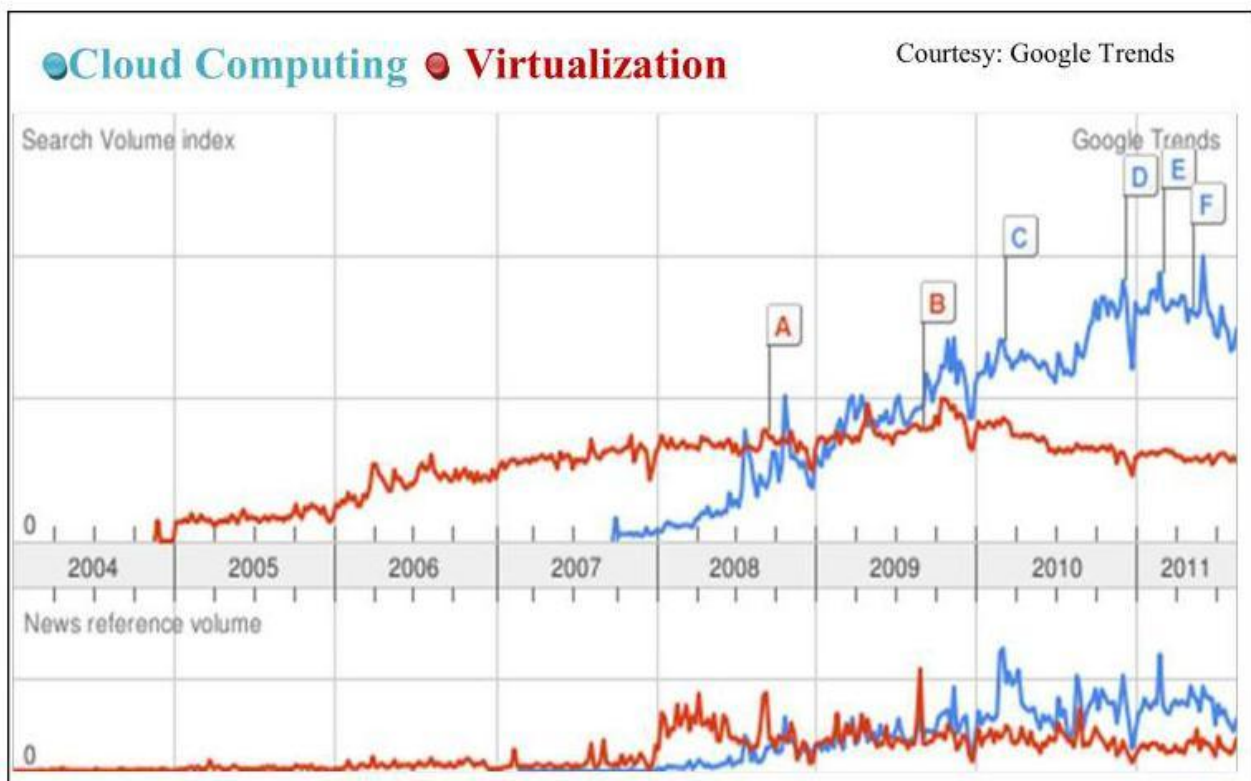


Figure.2.7: Google Trends showing the searches on Cloud computing Vs Virtualization

## **2.7.1 KEY CHARACTERISTICS OF VIRTUALIZATION:**

Virtualization technology holds with some important characteristics. These characteristics are as follow:

### **2.7.1.1 INCREASED SECURITY:**

By introducing a new layer of virtualization in between the guest and the host, the level of security has increased. The operations of guest are generally performed on virtual machine. Virtual control manager manage the all activity of guest user on cloud in this way cloud is prevented by harmful operation performed by guest.

### **2.7.1.2 MANAGED EXECUTION:**

Virtual machine manager is responsible to manage all task assigned by guest. The virtual machine manager is also responsible for managing the resources required by task which are assigned by users or guest. There should have no problem with their virtual machines and resources used by those machines.

### **2.7.1.3 PORTABILITY:**

Portability is considered into the hardware virtualization and programming level virtualization. In the case of hardware virtualization guest feels like a virtual image means every guest is assumed as they have their own physical machine. But in the case of programming level virtualization there is no need to recompilation while running different programs from many number of guests.

## **2.7.2 VIRTUALIZATION TECHNIQUES:**

There are two main virtualization technologies in cloud.

### **2.7.1 FULL VIRTUALIZATION:**

Entire system is virtualized means whole operating system is virtualized on virtual environment Like VMware, corresponding virtualized chunk of memory and hdd. It seems like all entire system is running on raw hardware and virtual machine looks like single physical machine assigned to guest.

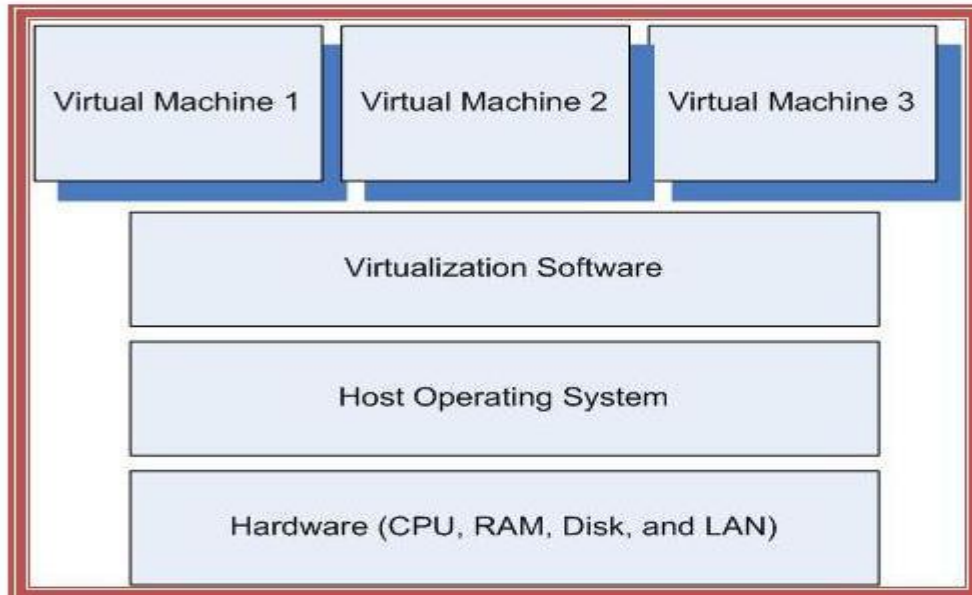


Figure 2.7.1

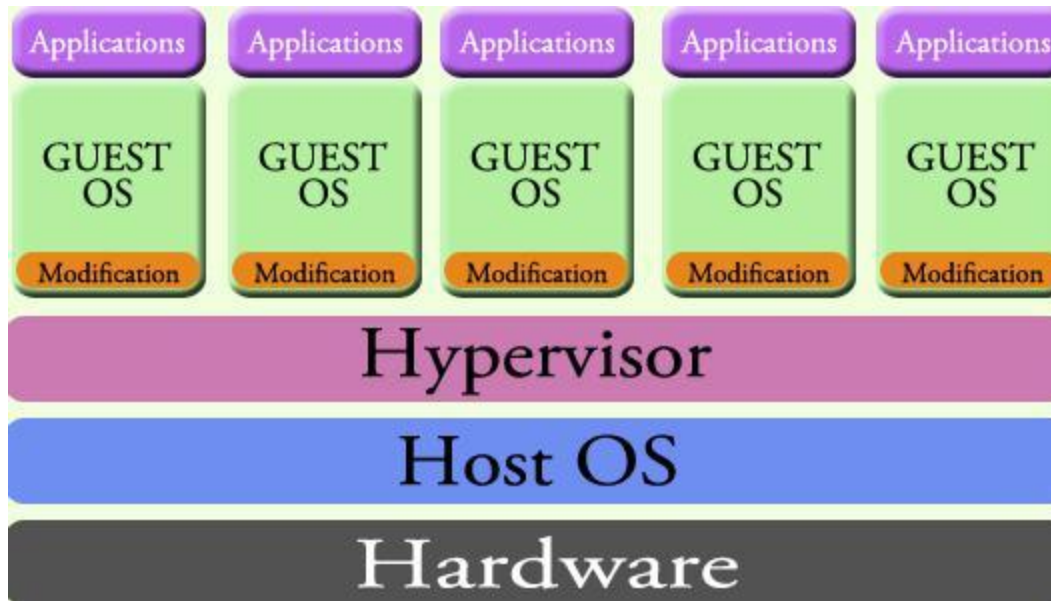
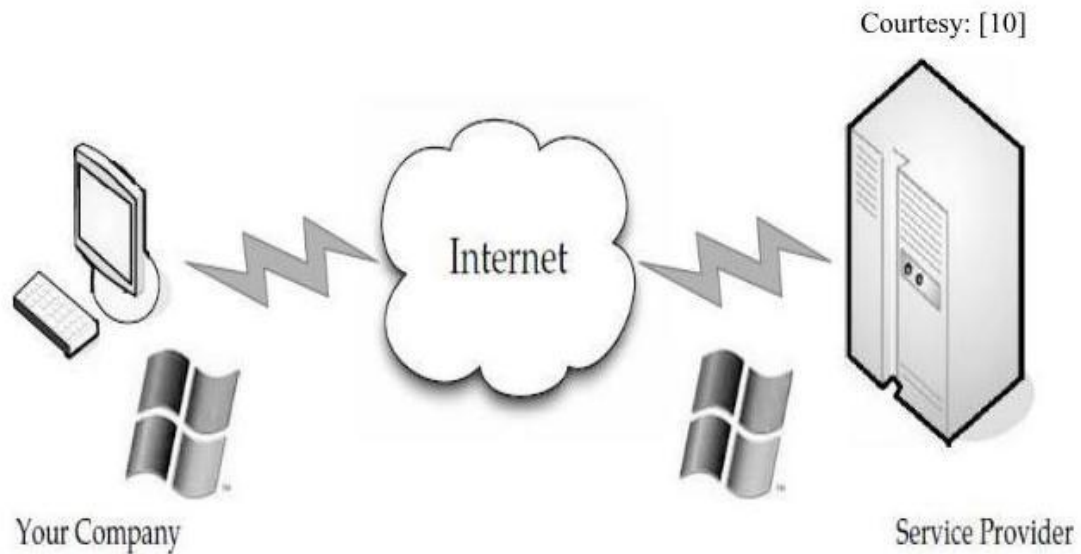


Figure 2.7.2



In a fully virtualized deployment, the software running on the server is displayed on the clients.

Figure.2.8: Full Virtualization

### 2.7.2.2 PARA VIRTUALIZATION:

This technique is useful in case of disaster recovery, migration from one system to another system and capacity management. It allows multiple operating systems to run on underline hardware at the same time by making it more efficient. The para virtualization module such as hypervisor or virtual machine monitor operates with an operating system which has modified to work in a virtual machine. Full virtualization emulated the whole system that is BIOS, HDD, Processor, and NIC. Therefore in Para virtualization operating system will have better performance than full virtualization which emulates all elements. Para virtualization is more efficient and security but at cost of flexibility. Flexibility is lost in Para virtualization reason behind it, OS must be modified to run with Para virtualization means a particular OS cannot be readily available for solution. Like window, Linux, Red hat server may not be available to the guest OS for a particular solution.

### 2.8 ISSUES IN CLOUD COMPUTING:

There is some issue related with cloud computing that is surveyed by researcher as follow:



### **2.8.1 SECURITY:**

With emergence of cloud technology which is at boot in market of storage and computational task at lower cost. At any component there can be security problem such client side, at transmission channel, at server side etc. Almost cloud is able to deploy any infrastructure of company for which company has to pay .At every layer cloud is able to provide services to their customer at software or application types service, at development level of service like it can provide the tool for developing software or any application. Infrastructure such as hardware, network and specific sever system but it is bitter true there is major security at every layer. Since business organization or any customer will think once before storing their on cloud because of sensitive data. More sensitive information is kept by business organization which can be their rich information for business logic processing or an important decision is taken by that organization based on their repository information. Defiantly cloud service provider should have satisfactory level security solution to make faith that data stored by cloud user is secure.

There can security issue in virtualization of cloud's component. Like an attacker can inject their harmful code into database of cloud or inject kernel code into os virtualization and can take control of all virtual machine which are used cloud providers.

### **2.8.2 PRIVACY:**

Since sensitive information is stored on cloud .It is okay with that nobody is able to see cloud user's data to except cloud service provider or one who managed user's data and can see their data. But point is how user comes to know that administrator is okay or their data is confidential when they lose their control from data now. So there is need of such technique which should not be dependent even on cloud administrator. Since on same virtual environment many virtual machines is provided to cloud user, may be this data can be scattered to other VM.

### **2.8.3 AVAILABILITY:**

Data availability should be of higher degree at any time and at any location. Cloud service provider should make sure that data availability will be from any location or system failure problem. During any operation availability of data should be ensured by cloud provider. There should not be data loss during accessing of data in any operations performed by user's.

### **2.8.4 INTEGRITY:**

Integrity of data means changes need to be done by only authorized entities and authorized way. Unauthorized person must not be able to modify the data. Unwanted change may not corrupt the data but also a malicious code can be inserted by attacker. This malicious can corrupt the sensitive information on system or may take control of that system if system is server. The modification of data is mostly found on transmission channel. So cloud service provider must be make sure that integrity of storage data or accessing data is preserved. Such as banking account number accessing from cloud storage or accessing of banking database to complete any transaction or performing operations then these information must consistent and must not modified by any third party or attacker. Interruptions in the systems, like a power surge may also be create some unwanted change in data.

### **2.8.5 RELIABILITY:**

The cloud server has same problem as that of resident server related with reliability of data.

Data must be reliable and recoverable from any loss and corrupt of data.

### **2.8.6 LEGAL ISSUE:**

There are various legal issues such as trademark infringement, sharing of owner data resources can create security problem in cloud computing. Sharing of data may lead scattering of data to other virtual machine that was assigned to someone. Since user's data is stored at many location to save data at any cost or for saving data from any natural disaster, may create problem with user when user want to change cloud provider or may want to delete the file. It must be ensure

by csp after changing or data deletion, data must have deleted from all location where data is stored by csp.

### **2.8.7 VENDOR LOCK-IN:**

Since some of services are built by some vendor, that may create problem during migration of user's data from one cloud to other cloud.

### **2.8.8 COMPLIANCE:**

Various rules pertain to usage and storage of data may need regular auditing and reporting to cloud users about their data.

## **CHAPTER 3:**

### **OVERVIEW OF CRYPTOGRAPHY & NETWORK SECURITY**

This era has big demand of cryptography and network security because of huge amount of daily database from business organization, institution, scientific organization, research data are need to be protected from any kind of unwanted changing which can destroy the fruitful of sensitive information. As in this science era there can't trustable on traditional way to promise sensitive information will be protected by one owner physically that may head of that department. Even it is not possible to do this. There is need of something advanced way that must not be relying on traditional methods. Network security is hardly required because without internet it can't be think about spreading of information, accessing some required information, to connect product and people in open market. The information that manage product is more valuable than product. A organization is known to be market because of their product uniqueness and uniqueness is due unique invention and information. So there is need of to protect information from third party at client side, at transmission medium at storage side if it is outside. Since there are many method has been developed to provide security is called cryptography in internet and network. Cryptography make data unreadable to other party, in this way data is protected by data owner o

One who takes this responsibility? The main component of information system security is Confidentiality; Integrity and Availability. Our cryptography work on the basis of these three components .Every cryptography algorithm must satisfy one of the above components of information system security. Sometimes more than one algorithm is required to satisfy above all three components. Component of information security is criteria for becoming a valuable cryptography algorithm.

### **3.1 SECURITY GOALS:**

There are three components to be considered that is Confidentiality, Integrity and Availability.

#### **3.1.1 CONFIDENTIALITY:**

Confidentiality or sometimes called privacy is hiding of data. To makes unreadable data for unauthorized party. It makes sure that data transmitted on medium is only readable by intendant users that are sender and receiver. There are many algorithm that provide confidentiality like many Symmetric algorithm AES, DES etc. and asymmetric algorithm such as RSA, Elliptical algorithm and many lightweight green algorithms .Unreadable format of data is called cipher.

#### **3.1.2 INTEGRITY:**

Integrity makes ensure that there will be no modification to actual information. It makes ensure information and transmission both is safe as original content. Collision on channel may lead lost or modification of transmitted data must be stopped to maintain the data integrity.

#### **3.1.3 AVAILABLITY:**

## **METHODOLOGY:**

---

Data must be available at anytime and anywhere to the users. This picture comes when data is stored on third party and owner need data for performing operations at any time must be available .The authenticated customer of organization must be able to access their data. Availability must not be affected by any failure such as power off problem disconnection problem, slow server response, discontinuity of third party manager. The unavailability of data is just a harmful for any organization. For example any business have taken PaaS cloud service, surely the daily work of organization will be totally depend on availability of PaaS services provider. So this component has high degree of role in information system. Unavailability means meaningless information and loss of money and time.

### **3.2 ATTACKS:**

These security goals confidentiality, integrity and availability can be threatened by security attacker. There can be many kind of security attack depend on type of information used.

Mainly there are two attacks in cloud computing.

#### **3.2.1 INSIDE ATTACKS:**

Attack done by insider or attack that is done by inside entities such as an attack by cloud service provider .User's data can be seen and modified by cloud service provider. Since, users belief at the cloud service provider for their security. Therefore blindly user belief on csp they don't know csp can alter the information data. User's information may be exploiting by the cloud service provider.

So there should have some technique that does not make user rely on cloud service provider to except only server should come for managed user's data. There should communication between cloud user and cloud servers.

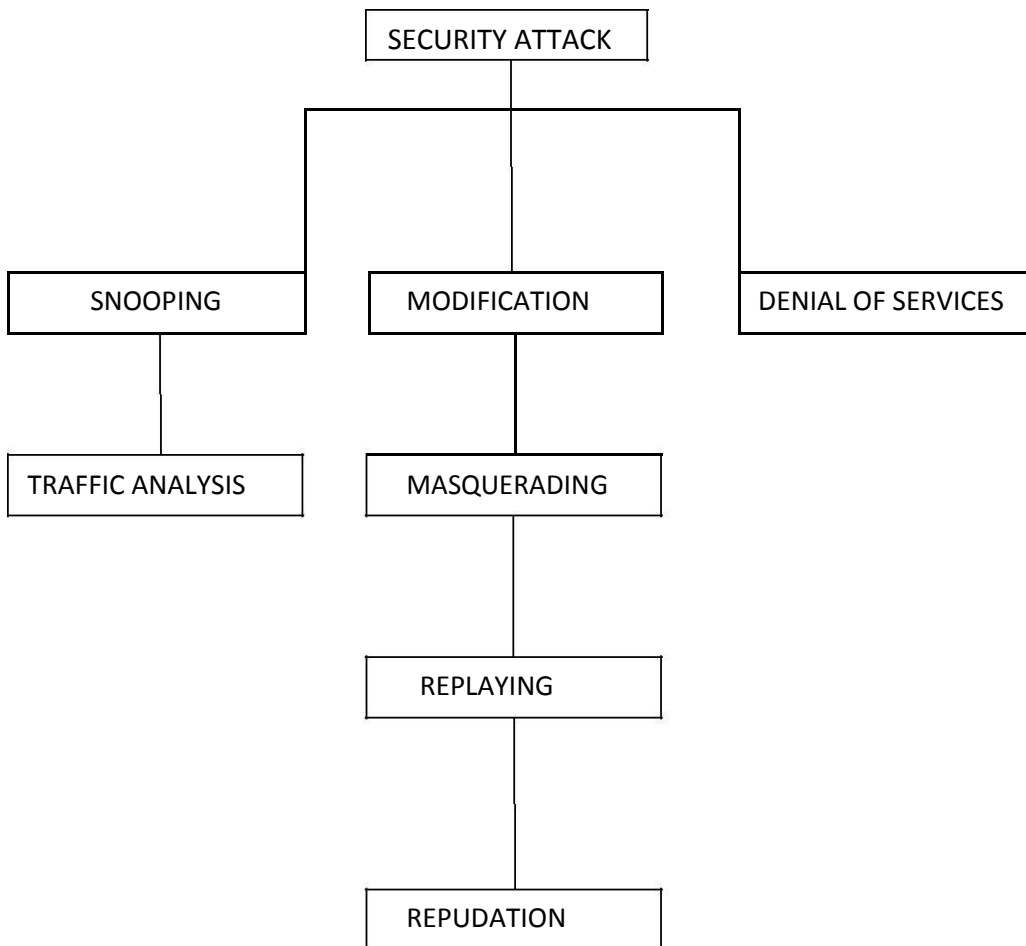
**3.2.2 OUTSIDE ATTACK:**

Attack is done by outside the organization not by cloud service provider, not by insider entities.

Malicious activity is done by outside people or unauthorized from outside of cloud.

**Taxonomy of attack related with security goal:**

Security attack is classified into three parts based on application in which attack is occurred and nature of attack.



**Figure 3.2.2**

Three classes of attacks are threatening to confidentiality; threaten to integrity, threat to availability. Attacker can attack at any level of cloud service model provided by cloud service provider.

### **3.3 THREAT TO CONFIDENTIALITY:**

There are two types of attacks threaten the confidentiality of data.

#### **3.3.1 SNOOPING:**

Snooping says there is unauthorized access to data or interception of data information. As example, a file data transferred through the internet may contain confidentiality information.

An authorized body may intercept and can use the information for own benefits. To prevent information from unauthorized entity then information must be in format of non-intelligible.

Information can be made non-intelligible by using encipherment technique.

#### **3.3.2 TRAFFIC ANALYSIS:**

Information can be made no intelligible for interceptor by using encipherment but still there is chance of getting other information related with transmitted information by online monitoring of traffic. For example an electronic address such email-id of sender or receiver may be detected by interceptor. Interceptor can collect couples of requests and responses that may help them to guess the nature of transaction.

### **3.4 ATTACK THREATENING TO INTEGRITY:**

## **A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:**

---

There are four types of security which are threatened in integrity of information.

### **3.4.1 MODIFICATION:**

After accessing data, an attacker can modify the data to make it beneficial to itself. Let say bank customer sends a message to bank for some transaction. Attacker can modify the type of transaction for benefits to itself or harm to the system. Sometimes attacker delays the message or can delete, to harm bank system or to take benefits from system. Many cryptography algorithms is there that make sure that data is not modified like strong diffie-Hellman and rsa signature to make sure there is no modification in data. Signature is method that provides prevention towards any kind of modification too data. If data is key for ciphering the data file of user then it became very necessary to encrypt the keys also. Most of symmetric algorithm uses the diffie-hellman with strong signature to make sure key will not be modified or read by attacker.

### **3.4.2 MASQUERADING:**

An attacker can impersonate the customer. Attacker can steal user valuable information such as the bank card and bank pin id of a bank customer and behaving like that one is bank customer this card and id. In this customer money can be stolen. An attacker can use fake ide to attack, like network identity, to gain unauthorized access to personal computer pretended as legal access of data. They try to steal user password by a program gap or fake login page or authentication process. An insider attacker may use key logger for stealing password, or if administrator leave any system open then attacker can take benefits to it.

### **3.4.3 REPLAYING:**

These types of attacker obtain a copy of message transmitted by a user and then try to replay it. For example a bank customer sends a request to their bank to ask for payment to attacker but



## **A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:**

---

Attacker has done their job. Attacker can intercept the message can send it again to receive another payment. Replaying can take more benefits when key is sharing through transmission media.

### **3.4.4 REPUDIATION:**

Repudiation is happened when any one of entity either sender or receiver deny their message which are sent or received by them. Sender of message may deny that message is not sent by them and receiver of message might deny that message is not received by them. For a bank customer first request to their banking system to make a payment to third party and after payment done by bank, customer deny that nothing such request was made by him. For denial of receiver can be understand by example, suppose receiver buy a product from a manufacturer and paid for that ,manufacturer receiver payment and later on deny to receiving of payment and again ask to be paid.

## **3.5 ATTACKS THREATENING AVAILABILITY**

### **3.5.1 DENIAL OF SERVICE:**

It is very common network security attack. It may slow down the system service or totally interrupt the system service. An attacker can used many strategies to achieve this goal. They can send so may bugs report to server to slow down the server access by clients and client will think server is not responding them. An attacker could delete server response to a client and make a feel to client that server is not responding their request. Attacker may modify the clients requesting and causing it, client can send so many requests and lastly server can get heavy load.

## **3.6 OTHER CATEGORY OF ATTACKS:**

### **PASSIVE VERSUS ACTIVE ATTACKS:**

# A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:

Attacks can be classified into active and passive attacks by following tables.

## Passive Attacks

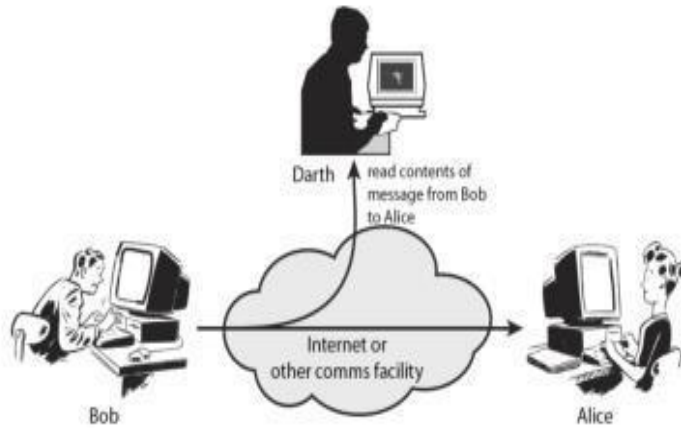


Figure 3.6

## Active Attacks

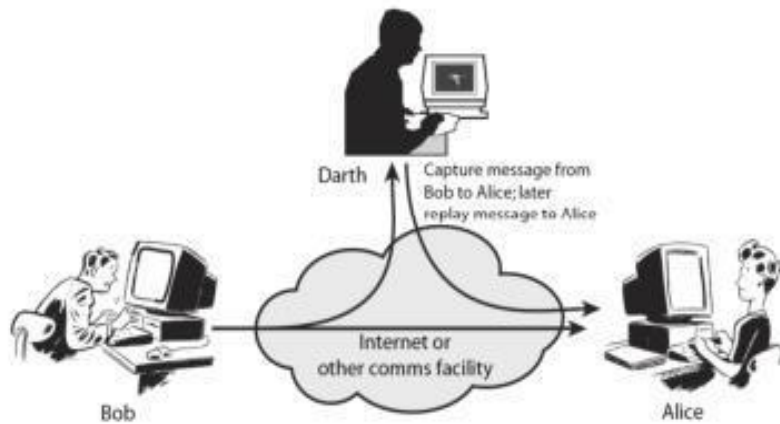


Figure 3.6

ATTACKS	PASSIVE/ACTIVE	THREATENING
Traffic Analysis Snooping	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Dos(Denial of service)	Active	Availability

**Table 1**

### **PASSIVE ATTACKS:**

The attacker looks for only obtaining information in this attack. Means data is not modified by attack and also system is not harm by attack. System being work its normal operations but Attack may harm receiver and sender of transmitted message. Senders and receivers might be harmed but system shall not be harmed. That's why it becomes very difficult to identify the type of attack until receiver and sender of message finds out about the leaking of confidential data. Passive attack can be cure by encipherment of the data.

### **ACTIV E ATTACK:**

Active attack can change information or harm the system. The attacks that threaten the integrity and availability of data are known to Active Attack. This attack is normally easier to find out

## **A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:**

Than to prevent, because of attacker may launch attack in a various way. Active attack is more harmful than passive attack because of passive attack does not affect the server operation or server system while active attack may harm the system so it becomes easier to detect the attack; detection of attack is more powerful by server rather than simple intendant sender and receiver of message.

### **3.7 SECURITY SERVICES AND MECHANISM:**

ITU-T (International telecommunication union-Telecommunication standardization security) provides some security services and mechanism to implement those services.

#### **3.7.1 SECURITY SERVICES:**

Mainly five services are provided by ITU-T.

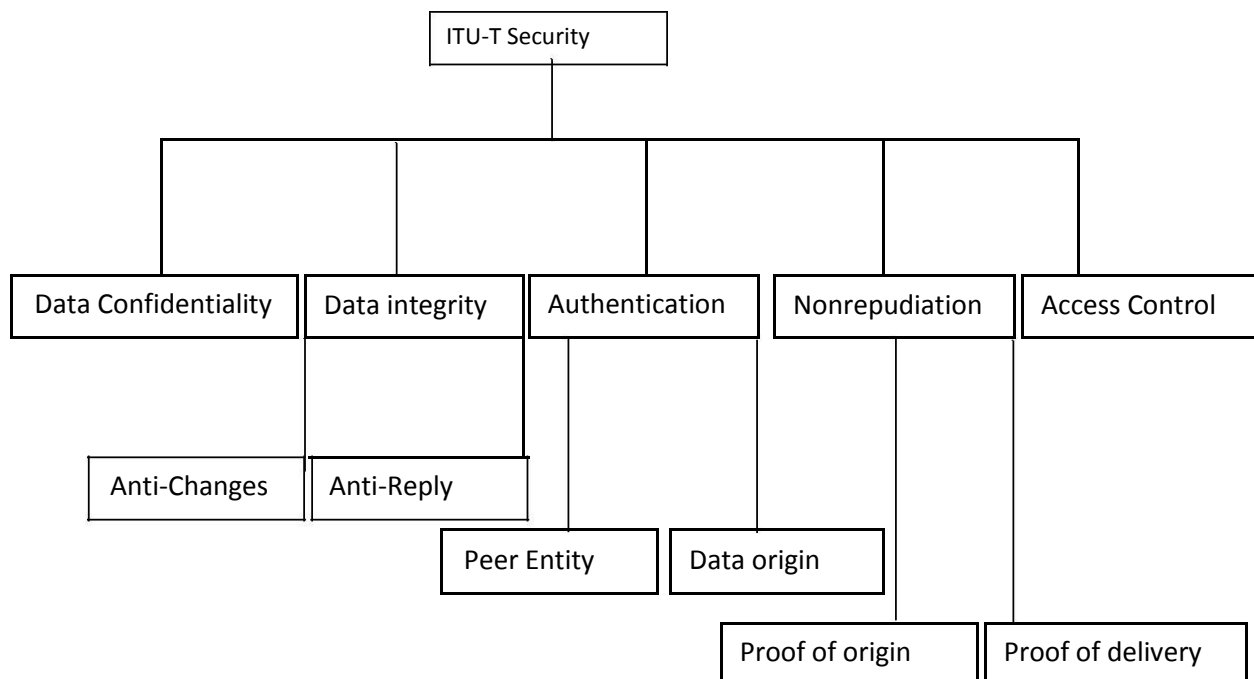


Figure 3.7.1

### **3.7.1.1 DATA CONFIDENTIALITY:**

It is designed to prove privacy over data or making information unreadable to other than receiver and sender. It is designed stop snooping and traffic analysis types of attack.

### **3.7.1.2 DATA INTEGRITY:**

Its design purpose is to protect information from alert nation, insertion, deletion and replying by an attacker.

### **3.7.1.3 AUTHENTICATION:**

It provides identity between sender and receiver to protect from fraud communication. In connection oriented Communication, it provides authentication of receiver and sender during their connection establishment. In connectionless communication, it authenticates origin of data.

### **3.7.1.4 NONREPUDIATION:**

It provides protection against by ether receiver and sender of message. Receiver of message can proof of receiving data when sender deny and by proof of delivery a sender can proof what is delivered by them when receiver deny that this data is delivered by intendant sender.

### **3.7.1.4 ACCESS CONTROL:**

It provides protection against unauthorized access to message.

## 3.7.2 SECURITY MECHANISM:

ITU-T also provides the security mechanism corresponding services that it is listed.

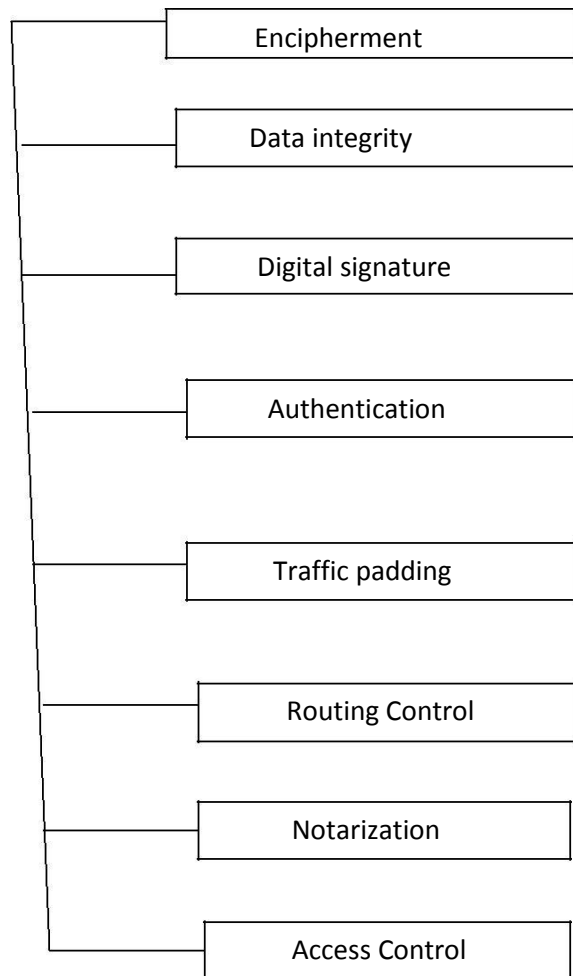


Figure 3.7.2

### 3.7.2.1 ENCIPHERMENT

Hiding of data can provide privacy or confidentiality of data. To make meaningless or unreadable to the party is known as encipherment. There two techniques which are allowed to provide encipherment, i.e. cryptography and steganography.

### 3.7.2.2 DATA INTEGRITY:

Data is appended with some check value which is created by data itself. When data and check value is received by receiver, receiver creates new check value using received data and then compare with both check value, if both has same value means integrity is preserved, if not same then it is supposed, data has been alerted. It just like message digest that also provides integrity where sender calculate hash value using original message called message digest and send message digest and data to receiver, receiver calculate its own message digest and match with received one, if same means there is no alternation in data.

### **3.7.2.3 DIGITAL SIGNATURE:**

It is a means by which sender creates electronic sign the data and receiver electronically verify the signature such as sender signed the document using its own private. Now receiver will receive the document and receiver use sender's public key to prove that data message is really signed by sender or some else.

### **3.7.2.4 AUTHENTICATION EXCHANGE:**

Two body exchange message to prove their identity to each other.

Authentication means sender must aware with receiver to whom, message is sending because receiver can be a fraud. Receiver has to be also identifying from where data is coming, because it may come from fraud or attacker. To access any database or website information their customer has to be login first is also a part of authentication.

### **3.7.2.5 TRAFFIC PADDING:**

To prevent from any adversary's attempt, communicating entities insert some bogus data into transmission traffic.

### **3.7.2.6 ROUTING PROTOCOL:**

It means every time change routing route a select a different route from available route between sender and receiver to prevent harmful attempt from eavesdropping on a particular path.

### **3.7.2.7 NORMALIZATION:**

Normalization means to select third party to manage the communication between two entities.

### **3.7.2.8 ACCESS CONTROL:**

Access control means customer verification by password and pin\_id.

### **3.7.2.9 RELATIONSHIP WITH SERVICE AND MECHANISM:**

Mechanism corresponding services can be shown by this table.

Security Service	Security Mechanism
Data Integrity	Data integrity, Encipherment, Digital Signature
Data Confidentiality	Encipherment and Routing Control
Authentication	Authentication exchange, Digital signature, Encipherment
No repudiation	Normalization, Data integrity, Digital Signature
Access Control	Access Control Mechanism

**Table 2**

## **3.8 CRYPTOGRAPHY:**



## A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:

---

It is an art of transforming the message unreadable to protect from attacker. Means, an encryption and a decryption of message using secret key. It includes encryption, decryption and hashing.

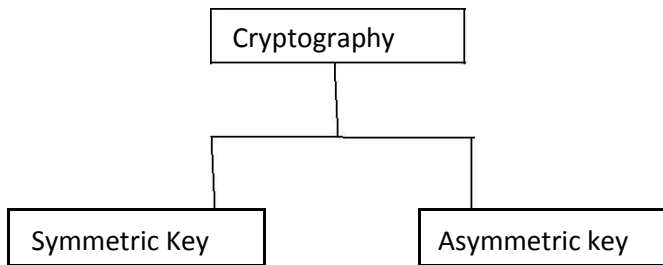


Figure 3.8

### 3.8.1 SYMMETRIC-KEY ENCIPHERMENT:

In symmetric key, encryption and decryption are done by similar key. Means same key is used for both encryption and decryption.

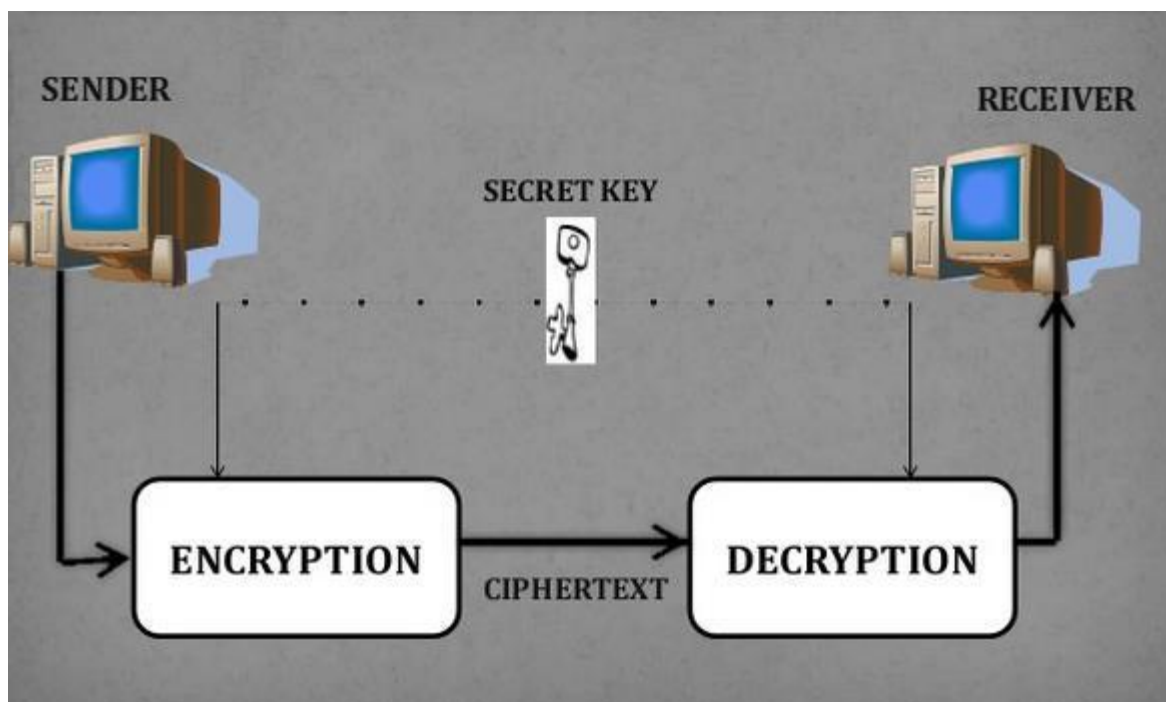


Figure 3.8.1

Here the same key is used by both. Sender encrypts data using this secret key and receiver decrypt the data using same secret key.

### 3.8.1.1 TRADITIONAL SYMMETRIC-KEY CIPHER

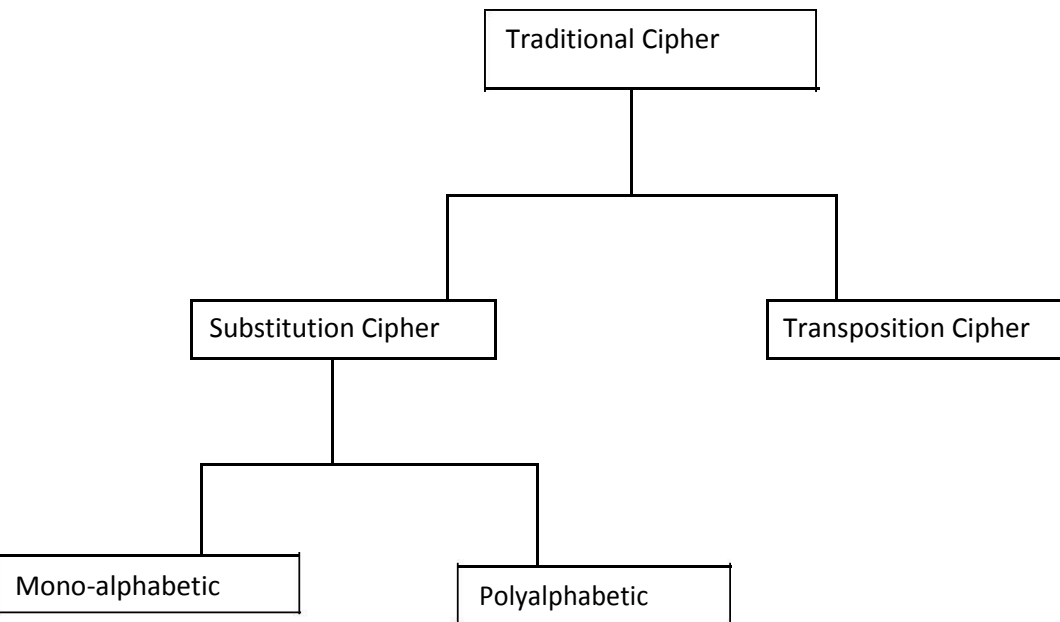


Figure 3.8.1

Traditional cipher is character-oriented.

#### 3.8.1.1.1 SUBSTITUTION CIPHER:

Replace a symbol with another symbol.

#### 3.8.1.1.2 Mono-alphabetic substitution cipher:

A character in plaintext is always replaced with same character in cipher character without worry about position.

## **A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:**

---

For example if algorithm is about A has to be replaced with E then every A in plaintext must be replaced E in cipher text. There is one-to-one relationship of character between plaintext and cipher text.

### **3.8.1.1.3 Polyalphabetic substitution cipher:**

Each occurrence of a symbol can have different substitute. Means relationship between a character of cipher text and a character of plaintext can have many-to-one.

For example a character may substitute by E in first occurrence but may substitute by L in middle. But point is since there is one-to-many relationship between a character of plaintext and a character of cipher text how to map cipher to plaintext during decryption at receiver side. It obvious that the key must make clear which of possible character can be chosen for encryption.

### **3.8.1.1.2 SHIFT CIPHER (Ceaser cipher):**

The simplest mono-alphabetic substitution is Shift cipher. Every character of plaintext if it is one case, would be replace by some n number position down character and at time of decryption ,every character of cipher would be replaced by same n number of position up character.

### **3.8.1.2 TRANSPOSITION CIPHER:**

It is position oriented cipher no substitution take place. Position of a character in plaintext can be at different position in its cipher text. Transposition cipher reorders the plaintext in a block of character.

There is a key that is used to mapping between positions of the character between plaintext to cipher text. It is very clear that bijective function is used to encrypt the plaintext while inverse function is used for decryption.

There are many types of transposition cipher:

RAIL FRENCE CIPHER: Plaintext written downward successive as a rail, KEY—"RAILS"

## A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:

---

“WE ARE HERE JUST BECAUSE OF YOU”

W . . . E . . . E . . . T . . . A . . . O . . . U  
. E . R . H . R . J . S . B . C . U . E . F . O .  
. . A . . . E . . . U . . . E . . . S . . . Y . .

CIPHER TEXT: WEETA OUERH RJSBC UEFOA EUESY

ROUTE TRANSPOSITION CIPHER:

PLAINTEXT----- → WRITE INTO GRIDE FORM-- → FUN  
(ROTATE/MOVEUP/MOVEDOWN/SPIRAL) → CIPHER

Example:

Plaintext:

W M I O R F E O E  
E E S V E L A N k  
A D C E D E T C Z

EKZCTEDECDAEWRIOMFEONALEVSE

**COLUMNAR TRANSPOSE :**

**Transposition Cypher (Example)**

PLAIN: F O U R S C O R E A N D S E  
V E N Y E A R S A G O

1	2	3	4	5		3	2	4	5	1
F	C	N	E	R		N	C	E	R	F
O	O	D	N	S	→	D	O	N	S	O
U	R	S	Y	A		S	R	Y	A	U
R	E	E	E	G		E	E	E	G	R
S	A	V	A	O		V	A	A	O	S

CYPHER: N C E R F D O N S O S R Y A  
U E E E G R V A A O S

**3.8.1.2.1 DOUBLE TRANSPOSITION:**

A single columnar transposition can be attacked by guessing to writing it into column then try to find all anagrams. So to make it stronger, double transposition cipher can be used with different key.

**3.8.1.2.2 MYSZKOWSKI TRANSPOSITION:**

It is an invariant columnar transposition that needs a keyword with repetitive letters.

Key: POTATO its number string let say "432143."

GRID FORM OF INPUT: "WE ARE HERE JUST BECAUSE OF YOU"

4 3 2 1 4 3  
W E A R E H  
E R E J U S  
T B E C A U  
S E O F Y O  
U

CIPHER:

"RJCF AEE0 ERBE WETSU EUAY HSUO"

**3.8.1.2.3 DISRUPTED TRANSPOSITION:**

## A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:

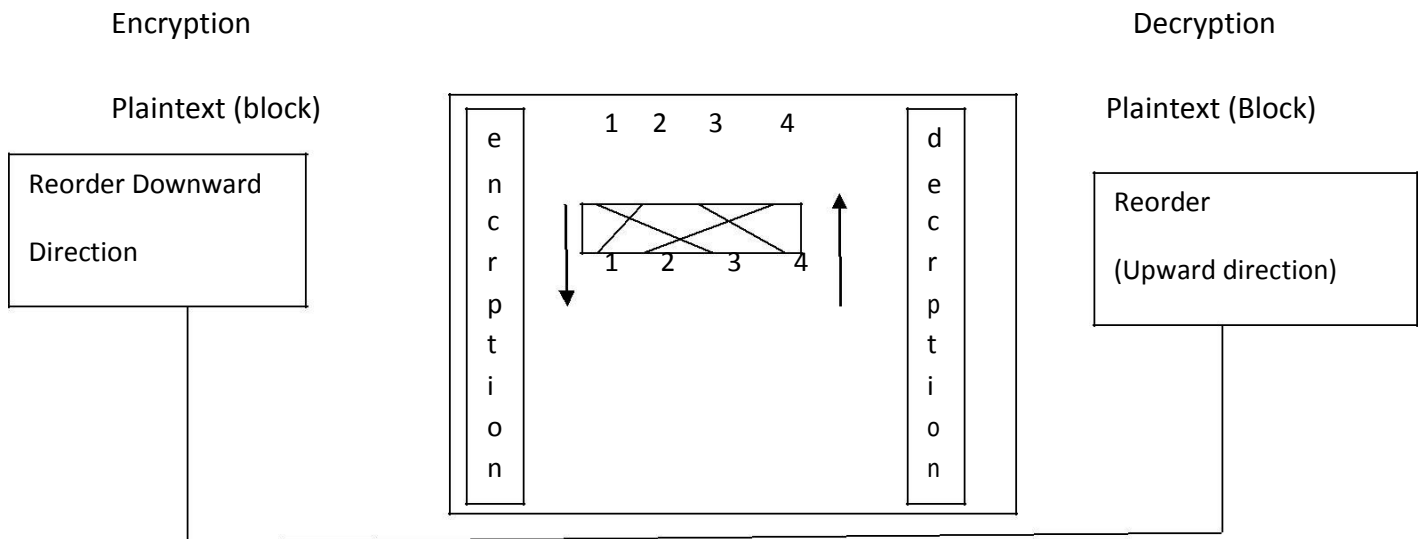


Figure 3.8.1.2.3

### 3.8.1.2.4 SIMPLE MODERN CIPHER:

Traditional cipher is character oriented. While computer need to be bit-oriented. Data can of any form such audio, video, number, graphic, image etc. So this very clear that our encryption and decryption should base on bit oriented because computer store or do any operation on bit value of message. So every character that has one byte converts into its equivalent binary bit for performing security.

**There are many types of Simple Modern Cipher.**

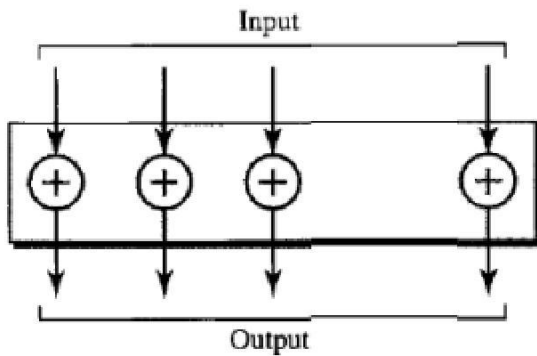
### 3.8.1.2.5 XOR CIPHER:

It takes two inputs then after x-or then cipher text is occurred.

Input:

Text, key

Cipher-  $\rightarrow$  text x-or key

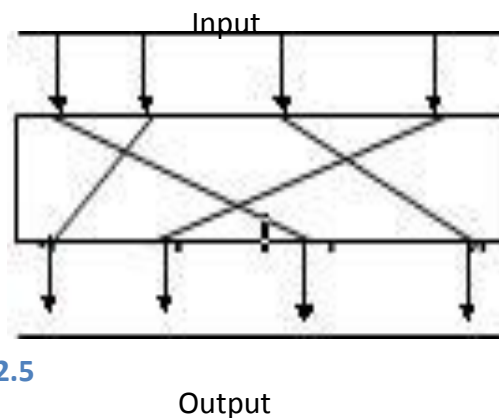


**Figure 3.8.1.2.4**

But remember the size of key must be equal to size of input.

**3.8.1.2.5 ROTATION CIPHER:**

Input bits are rotated left or right. It can be keyless or keyed. In the case of keyed rotation the value of key defines the number of rotations. While in keyless rotation the number of rotation is fixed, that means you can't change.



**Figure 3.8.1.2.5**

**3.8.1.2.6 SUBSTITUTION CIPHER: S-BOX**

S-box is keyless and used as intermediate stage of encryption and decryption. Its input can be length of n but output can be length of m, it is not necessary to be equal of n and m. The function that matches input and output may be defined as table.

## 3.8.1.2.7 TRANSPOSITION CIPHER: P-BOX text

A p-box i.e. permutation box works for bits parallels the character of the traditional cipher. It transposes the bits of input bits of input.

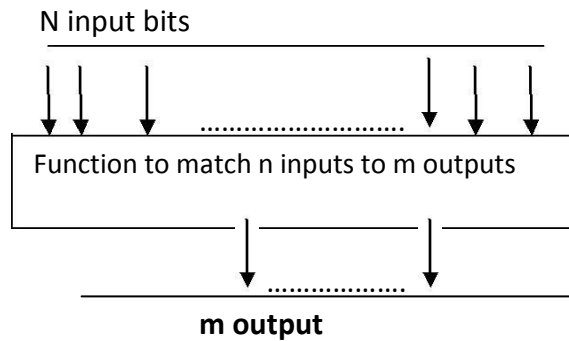


Figure 3.8.1.2.7

It can be implemented in both hardware and software but is faster in hardware. Like s-box, p-box is also keyless. There are three types of permutation as follow

## 3.8.1.2.8 Straight p-box Permutation:

In this straight permutation the number of inputs is equal to number outputs.

Means if number of inputs is n then number of outputs will be also n. The shuffling does not s number input to number of outputs.

## 3.8.1.2.9 Expansion p-box Permutation's.

Number of inputs and number of outputs both will be different. Number of outputs is greater than input.

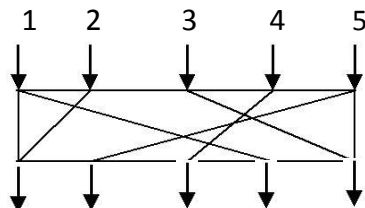


Figure 3.8.1.2.9



1 2 3 4 5

Straight

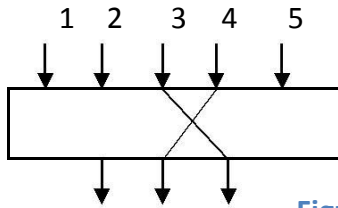


Figure 3.8.1.2.9

1 2 3

Compression

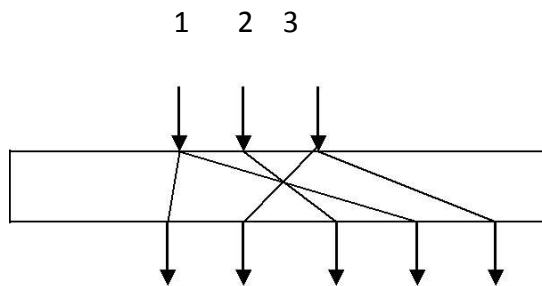


Figure 3.8.1.2.9

1 2 3 4 5

Expansion

**3.8.1.2.10 Modern Round Cipher:**

It involves the multiple rounds. At every round it produces the complex output. If there is n number of rounds then there will be n keys. Such for round 1, key  $k_1$ , for second round key  $k_2$ , and for second last key  $k_n$  are used. The modern cipher symmetric key algorithm such

## **A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:**

---

as DES and AES. This cipher is also known as block because plaintext is divided into the block before encryption or decryption. For encryption and decryption same key are used. For symmetric key algorithm, DES as follow

DES has two p-box rounds and 16 complex round .First round straight simple round and last round same as that of first and between both round, there will be 16 rounds. All 16 rounds are same but since them performance with different key so there will different out at every iteration of round. The first and last round both is keyless and inverse to each other.

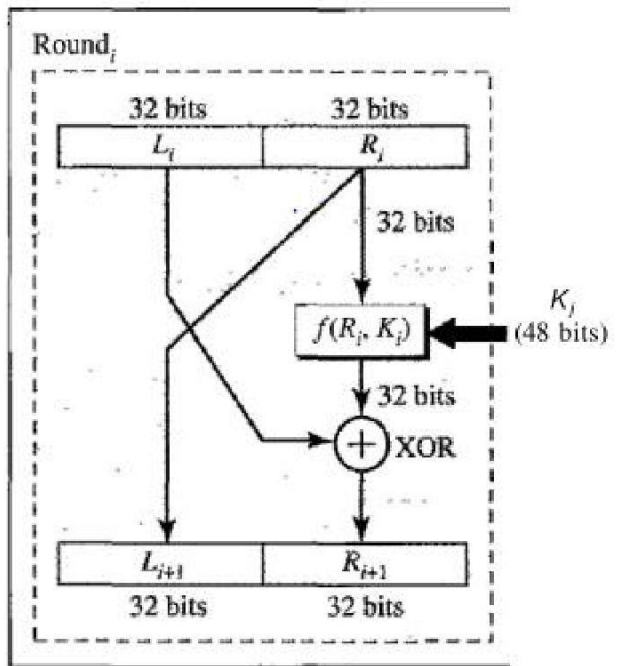
Permutation takes input of 64 bit. The structure of encryption and decryption both is different. Plaintext of 64 bit is divided into two blocks of 32 bit each second 32 bit will be copied to fist block of its output level and first (left) block of 32 bit performed operation with 48 bit keys. The DES functions apply 48 bit key with 32 bits rightmost that produces the 32 bits output and now this 32 bit output is x-or with leftmost 32 bits. After x-or the result is of 32 bits that will be copied to rightmost block of its output level.

The DES function is made of four operations that are an x-or, an expansion permutation, a group of S-boxes and straight permutation.

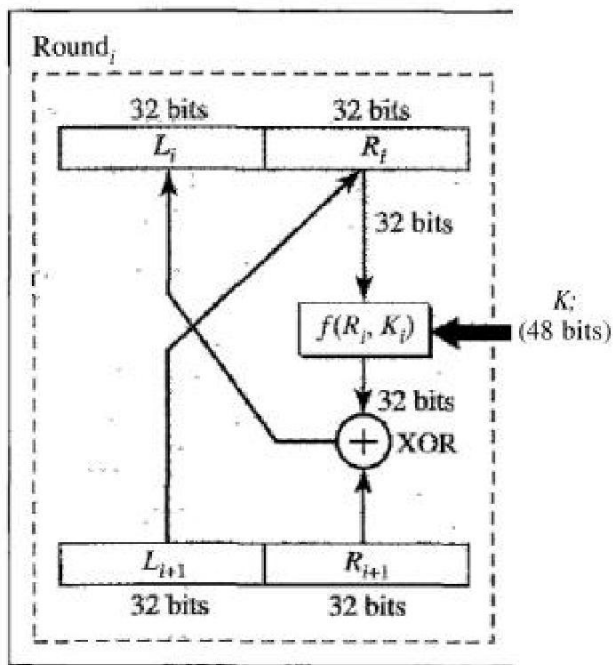
### **3.8.2.8 TRIPLE DES:**

In this DES algorithm, key size is too short. To increase the key size, 3-DES algorithm is proposed. There are two types of triple DES, Which is two keyed and three keyed.

The encryption block used as encryption-decryptions-encryption combination of simple DES. But decryption phase is combination of decryption-encryption-decryption. To make key size of 132 bits and to protect from man-in-middle attack, DES with 2 keys is used. In these two keys 3-DES has first and last is of equal. But still there is problem, key size so lastly AES algorithm is designed that has key of size 128 bits, 192 bits, and 256 bits. Each of



a. Encryption round



b. Decryption round

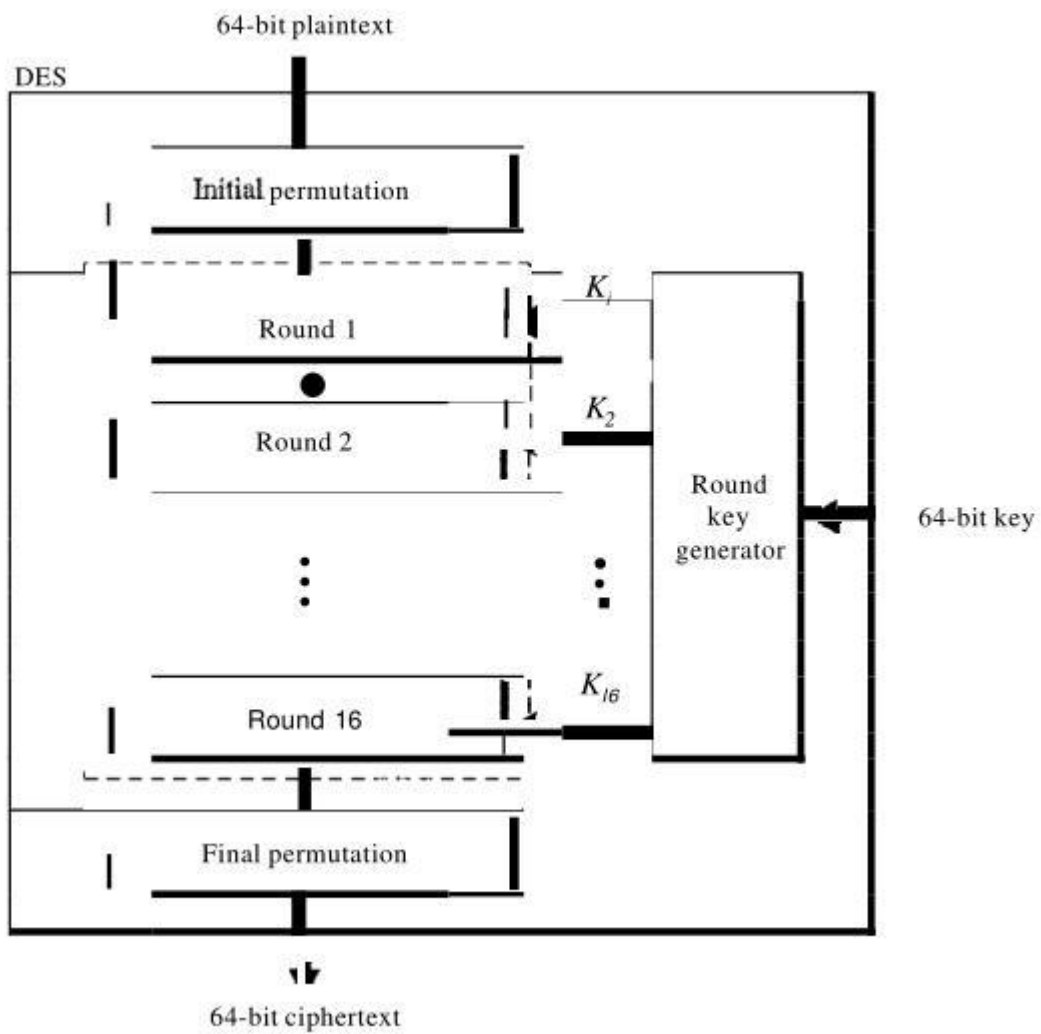
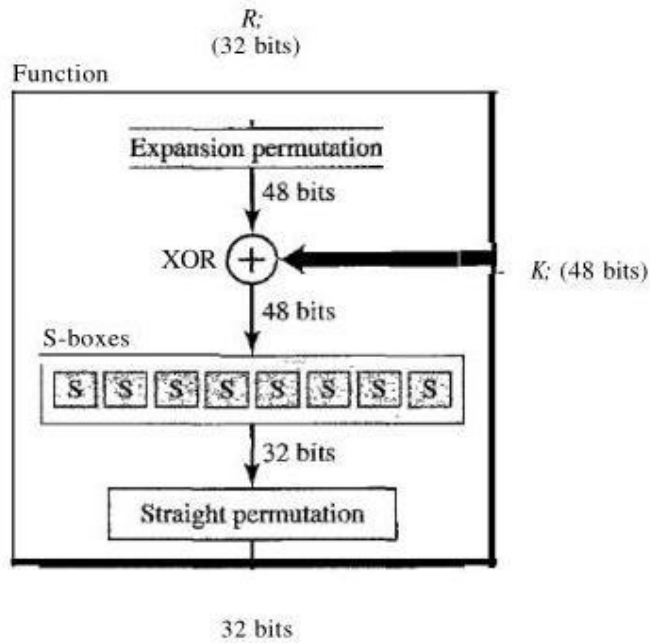


Figure 3.8.2.8

## A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:

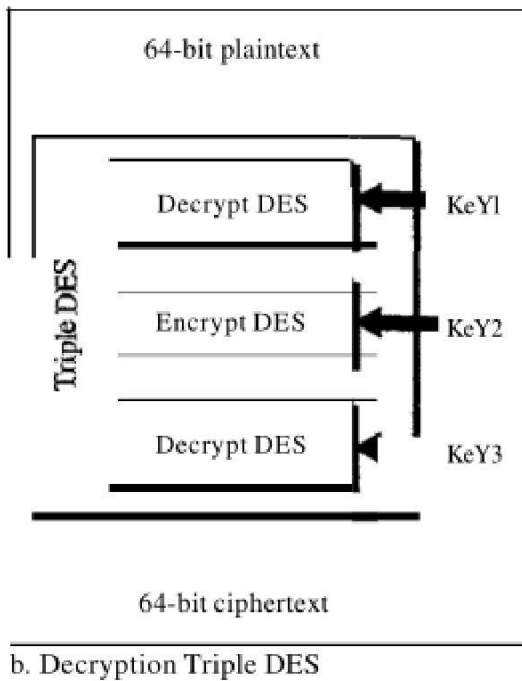
---



**Figure 3.8.2.8**

These key has different number of rounds, for 128 bits 10 round, for 192 bits 12 round and for 256 bits 14 rounds is used.

**A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:**



**Figure 3.8.2.8**

**3.8.2.9 AES (ADVANCED ENCRYPTION STANDARD):**

Its configuration is:

<i>Size of Data Block</i>	<i>Number of Rounds</i>	<i>Key Size</i>
128 bits	10	128 bits
	12	192 bits
	14	256 bits

**Table 3.8.2.9**

According to number of rounds and key size, AES has three different configurations. An x-or operation followed by ten round ciphers. Last round is little different from earlier nine one.

The structure of each round is as follows, first four has identical operation and last one has three identical operations. The output of previous stage is acts as the input for the next stage. At every time output becomes very complex. But 10 iteration blocks are almost identical. Let see the 128 bit key size AES. Most of the cipher has same characteristics of both DES and AES. Only difference is number of rounds and size of block.

## A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:

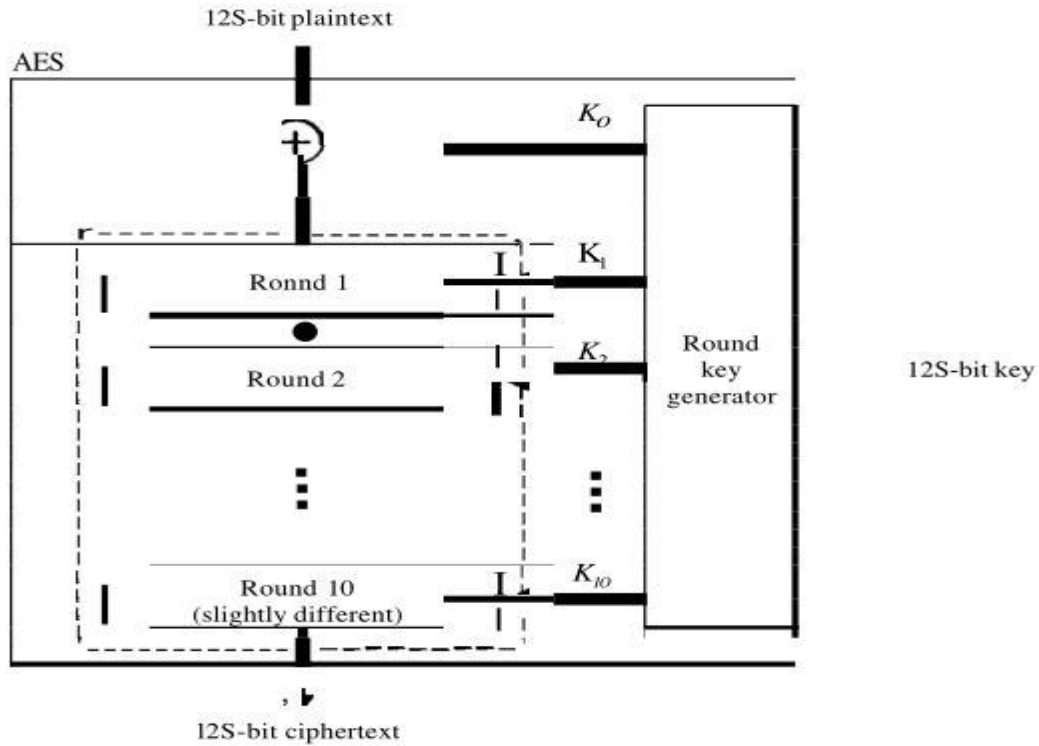
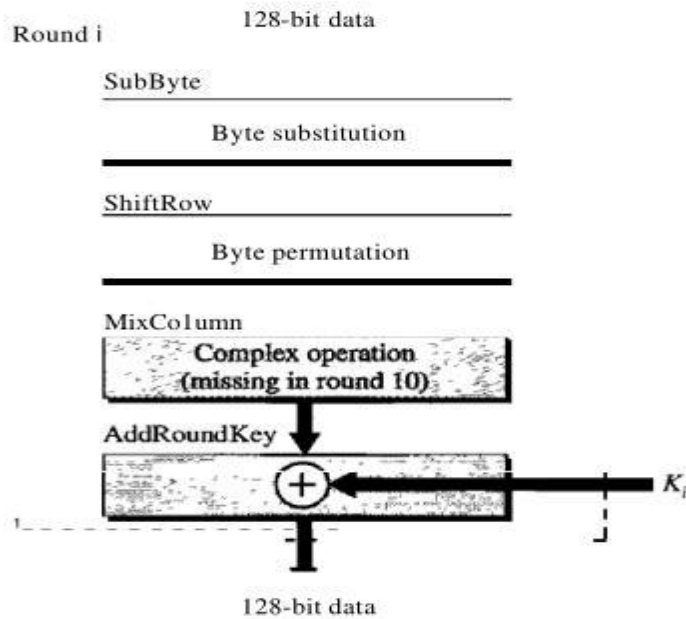


Figure 3.8.2.9



## **A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:**

---

There are some also algorithm that also comes into symmetric block cipher algorithm.

### **3.8.2.8.10 IDEA (INTERNATIONAL DATA ENCRYPTION ALGORITHM):**

Block size: 64 bits

Key size: 128 bits

It can be implemented in both hardware and software.

### **3.8.2.8.11 BLOWFISH:**

Block size: 64 bits

Key size: Between 32 to 48 bits

### **3.8.2.8.12 CAST-128(CARLISLE ADAMS AND STAFFORD TAVARES)**

Total rounds: 16bits

Block size: 64 bits

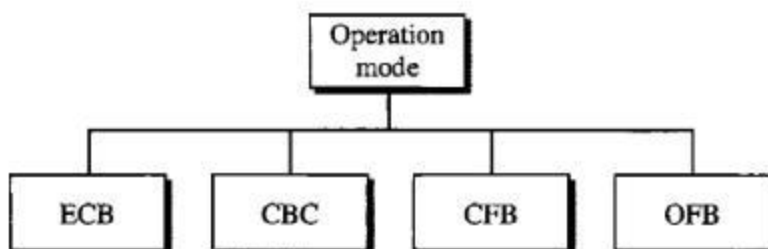
Key size: 128 bits

### **3.8.2.8.12 RC5:**

Designed by Ron Rivest

It works with different keys size, different number round and different block size.

### **3.8.2.8 .13 MODE OF OPERATION:**



**Figure 3.8.2.8 .13**



## A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:

### 3.8.2.8.14 ECB (Electronic Code Book):

If plaintext is of length  $N$  then cipher will be of also length  $N$ . Since the number of block in plaintext is exact the number of block in cipher text. Suppose 1,5 and 9 is the block of plaintext, it will be exact number in cipher. It is adversary, because the attacker can guess. Reorder of block in plaintext, may lead to reordering in cipher text. Each block is independent, so problem with one block does not affect the other block. Error in one block does not propagate to the other block.

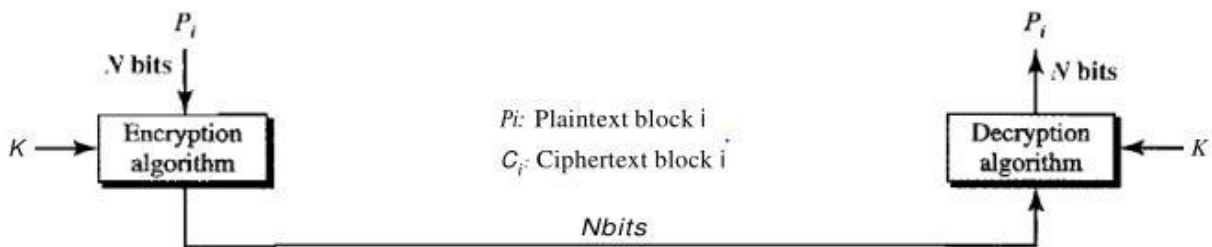
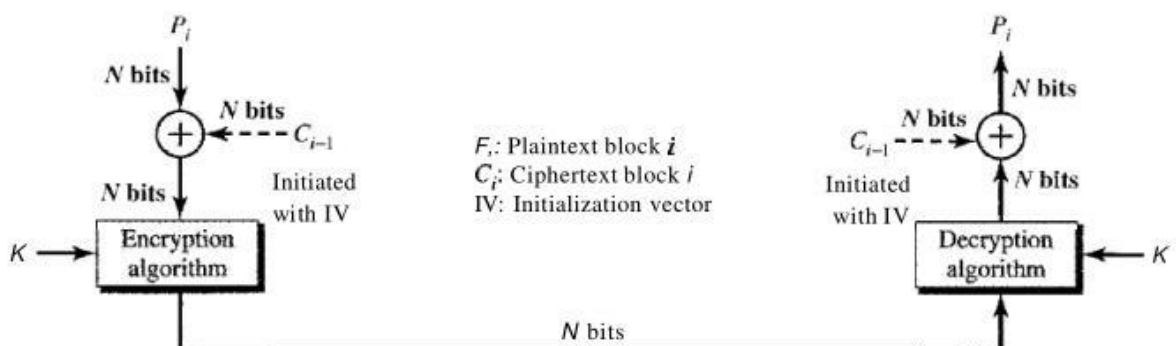


Figure 3.8.2.8.14

### 3.8.2.8.15 CBC (CIPHER BLOCKS CHAINING):

Each plaintext is x-or with previous cipher text block before being encrypted. When a block is ciphered, a copy of it is stored in memory to be used in encryption of next block.



# A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:

## 3.8.2.8.16 CIPHER FEEDBACK:

It is designed for especially those situations when there is need of send  $r$  bits of data where  $r$  is a just number that is different from block. Now problem is how to encrypt only  $r$  bits of data. The solution is encrypted, a block of bits and use only first  $r$  bits as key to encrypts the user  $r$  bits.

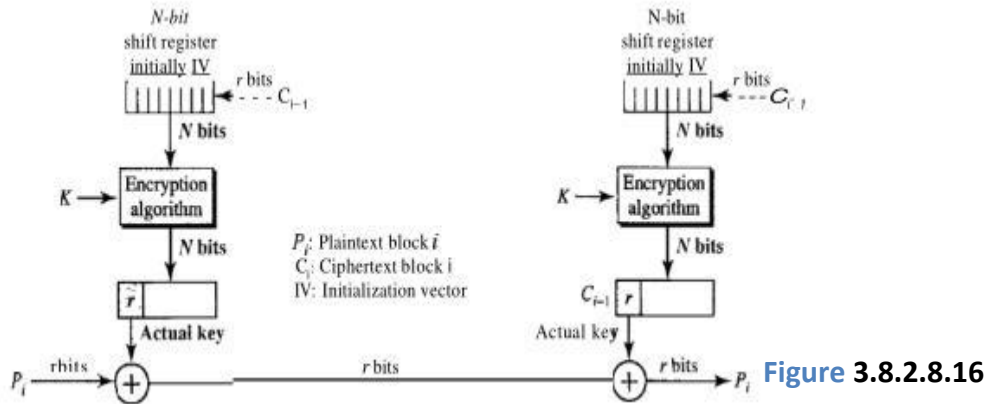


Figure 3.8.2.8.16

## 3.8.2.8.17 OUTPUT FEEDBACK:

Best part of this algorithm is that each bit of block independent. Block cipher like DES or AES is only used to create the key stream. Next bits stream is dependent on previous key stream. In creation of stream cipher text does not participated.

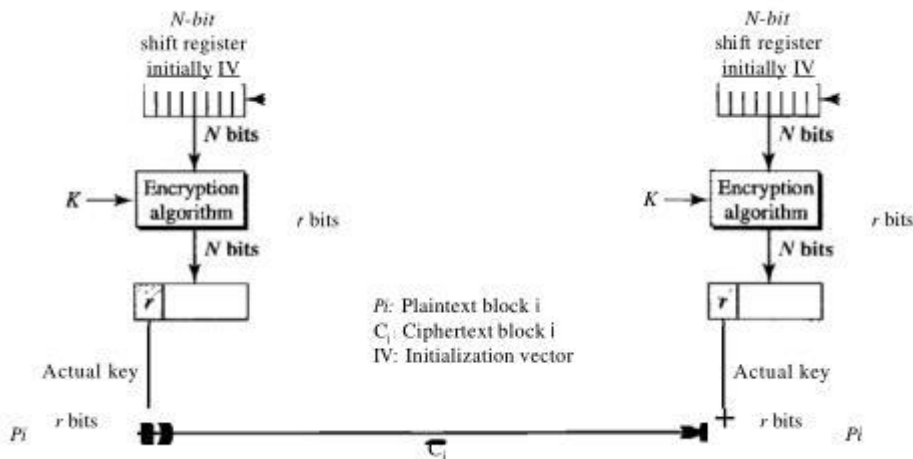


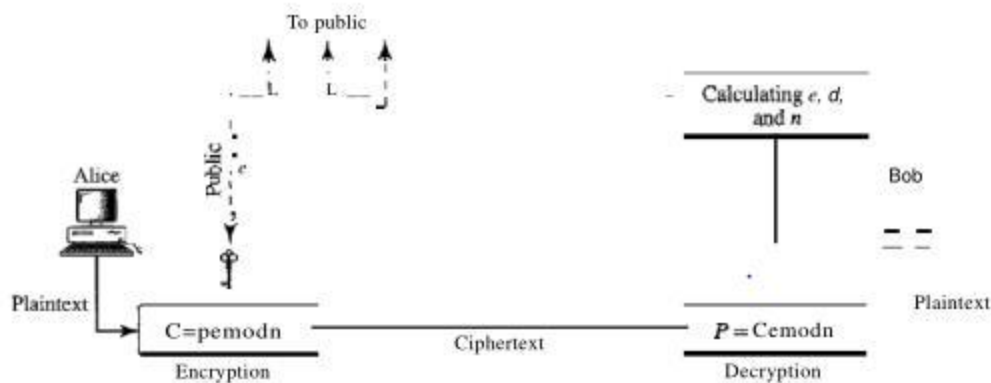
Figure 3.8.2.8.17

## A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:

### 3.8.3 ASYMMETRIC-KEY CRYPTOGRAPHY:

Different keys are used for both encryption and decryption in this algorithm. Different keys are used so it makes more strong security rather than symmetric key algorithm. But it takes more operational time than symmetric key algorithm. It is also known as public key cryptography.

Two keys are basically used that is public and private key. Where public is used for encryption and private key is used for decryption but only those can decrypt the data who have private key. Best and strongest example of asymmetric is RSA algorithm.



#### SELECTING KEY:

1. Bob chooses two prime number let say  $p, q$ ;
2. Bob calculate  $n = p \cdot q$ ;
3. Now Bob calculate,  $\phi = (p-1) \cdot (q-1)$
4. Choose  $e$  between 1 and  $\phi$ , s.t  $1 < e < \phi$ ;
5. Calculate  $d$  such that  $e \cdot d = 1 \pmod{\phi}$

Public:  $e, n$ ;

Private:  $d, n$ ;

Bob keeps private key to itself and announce public key publically. So any who want to send their data to bob then they can encrypt the message using public key that could be only encrypted by private.

## **A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:**

---

Encryption: plaintext p;

$$C=p^e \pmod n;$$

C is cipher text;

P must be less n; if large then it has to be divided in blocks.

Bob will encrypt the cipher C is:

$$P=C^d \pmod n;$$

### **Applications**

Since RSA can be used to encrypt and decrypt the actual data. It becomes very slow if message is very long. It is useful for short message like small message digest. RSA is used for digital signature and authentication.

### **3.8.4 DIFFIE-HELLMAN:**

RSA is asymmetric key cryptography that can be also used for encrypt and decrypt the symmetric keys. Diffie-Hellman is used for mainly key exchange.

It mostly used for symmetric key algorithm for exchanging their keys to keep secret from other to be known because same key is used for encryption and decryption. They have not to meet for key agreement. It will be done through internet.

Before establishing symmetric key, both parties have to choose two number p and g.

P is should be large prime number.

G is random number.

These two numbers are not necessary to keep confidential. These can be sent through internet.

It can be public.

# A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:

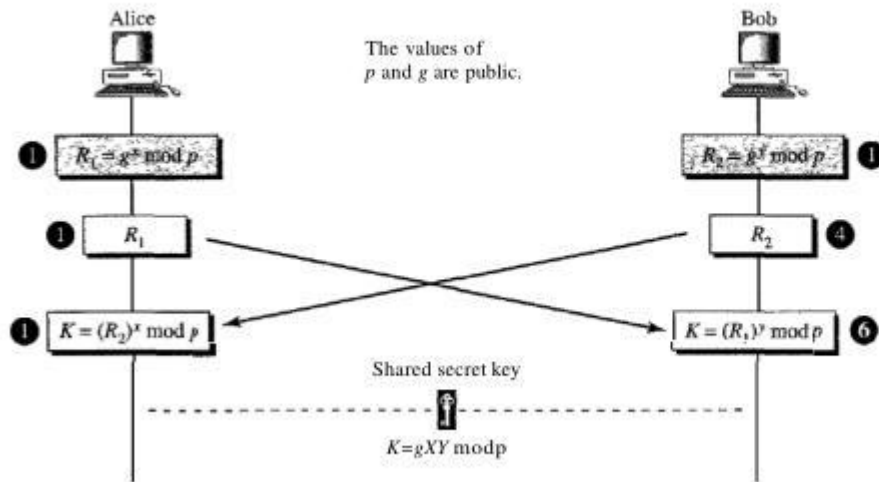


Figure 3.8.4

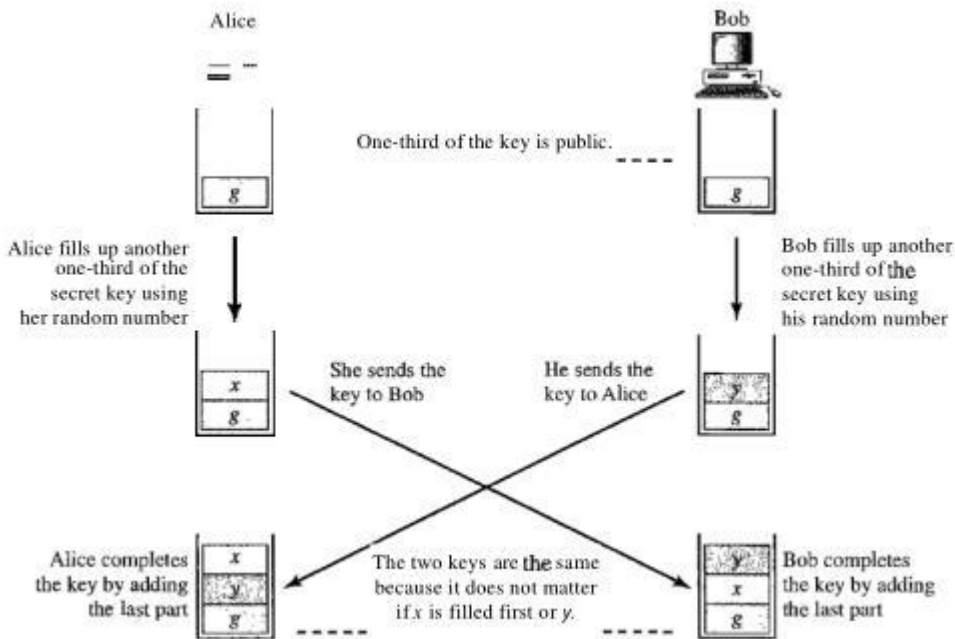


Figure 3.8.4

Attack can be avoided by authenticate to each other Alice and Bob. Sharing by diffie-hellman is needed to be used authentication for their right identification.

## CHAPTER 4

### 4.1 INTRODUCTION

A security system can have a lot of weak point like the place where cipher is stored, generating random number and strength of algorithm which is used. Cryptography can be classified in:

- A) Symmetric System: same key is used for both encryption and decryption. It works very fast and well for large quantities message .e.g. DES, AES, 3DES etc.
- B) Asymmetric System: It solves the key transmission problem of symmetric key cryptography. Depend on two keys public and private, public key is used for encryption while private key is used for decryption. Any can encrypt the message because of public is announced to all but only those may access have private key so safe journey of message without need of sharing of key by both parties as that of symmetric key algorithm. Not fast but difficult to break cipher. The common use is to encrypt and transfer a symmetric key. This is used by HTTP and SSL. Bad point is Asymmetric algorithms computationally very expensive. That's why combination of symmetric and asymmetric algorithm is used now a day for providing confidentiality, authentication and digital signature. Digital signature also ensures security. Signature is applied to whole message document. If signature is altered, the document becomes unreadable to anyone.

Since most of the cryptography depend on complex and hard computational mathematical methods. That's why a security is in need of to find new technology which does not rely on such pure mathematical method. Therefore, there should have alternative security cryptography system. Some algorithm those are accepted alternative security concepts are as Elliptical curve cryptography (ECC) algorithm, Vocal, Quantum, and DNA encryption algorithms. ECC is used for portable device which keeps limited processing power, use simple algebra mathematics and with small cipher. Quantum cryptography is methodology of creating and distributing private

## **A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:**

---

key. A gram of DNA amount can store  $10^{21}$  DNA bases that is equivalent to  $10^8$  terabytes of data. DNA is latest technology in cryptography based on their mathematical concept used in DNA. DNA has high level of computational ability and can store huge amount of data. A cryptography based on DNA splicing technique was OTP (one-time pads algorithms) algorithm.

Plaintext is combined with a pad using some modular operation or x-or them. To avoid the use of pure mathematical based symmetric and asymmetric algorithm, an advanced symmetric and asymmetric algorithm is bought that is DNA based cryptography.

Data encryption and decryption using DNA properties is proposed in 2012. It is the most recent and newer methodology for cryptography due to its capacity to store huge data and providing too complex cipher sequence of any kind of plaintext. It can be used as both Symmetric cryptography and as well as Asymmetric Cryptography. Much of the research work has been implemented based on DNA encryption technique. Most of the research work used DNA biological properties. DNA sequence consists of 4 alphabets A, T, G and C. Each of alphabets is nucleotides. DNA is sequence usually quit long. There are two DNA sequence as follow.

This is fist one segment of Litmus; it is actual length of nucleotides long;

ATGCAATCTGCACTGTGTCACATTTGCGG

CTGAGTCACGATTCGCGCTGAGTACAAT

TGTA ACTCAGCCGGAATTCCTGCAGCCC

CGAATTCGCGATTGCGGAGATAATTGTATT

TAAGTGCCAGCTCGATACAATAAACGCC

ATTTGACCATTACCACATTAGTGTGCAC

CTCCAAGCTCTCGCACCGTACCGTCTCTA

GGAATTCCTGCACGATATCTGGATCCACG

TAGCTTCCCATGGTGACGTCACC

Second one is segment of DNA sequence of the Balsaminaceae. Its actual length is of 2283 nucleotides long:

## A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:

---

TTATTATTATTTTCTTTTCATTTTTATCTCAG  
TTTCTAGCACATATCATTACATTTTAATTTT  
TCATTACTTCGATCATTCTATCTATAAAATC  
GATTATTTCTATCACTTATTTTTATAATTTT  
CAATATCCATCTAATGATTAGATTACATTA  
AAGAACTCGGTAAAAGAGACTAAACAT  
CAATCTAGAACAAGGCTTAGTTTATTTAAT  
GTATTATTTTATGTTATTTCTATTGACAAAT  
TAGTTAAGAGGCAAGTATCTGAGAT

The most beneficial point is that a large of number of DNA is publically available on various website. There are two methods which are used for encryption and decryption. First one is Binary coding scheme which used DNA base for cipher like (A 00), (C 01), (G 10), (T 11). Mean input if converted into integer as their ascii value then convert into binary then map above table content. Now first time cipher will be contains any number of A, C, G and T but the mapping table should be hiding, not to be publically available. Second one method is Complementary pair rule.

NUMBER	CORRESPONDIING LETTERS
0	A
1	C
2	G
3	T

Table 4.1

A, C, G, T is four nitrogenous bases which are used in to make strand of DNA.



A: ADENINE

C: CYTOSINE

G: GUANINE

T: THYMINE

Here plaintext will be encrypted into DNA sequence. Then cipher text will be decrypted using DNA decryption.

### 4.2 PROPOSED ALGORITHM:

#### (New DNA cryptography Technique)

This proposed algorithm is symmetric key algorithm.

It has three secret keys.

Some mathematical will be performed.

Encrypted data will be in DNA sequence.

It supports all ASCII character.

1. Three keys are taken here.
2. Key=(starting\_num, modulus, Hyphun\_indicesArray[])

3. Substitution\_arr: it will hold sequential integers. Array size is equals to length of plaintext. Example:

Substitution\_arr[i] = Substitution\_arr [i-1] +modulus;

4. Modulus: It is difference between each integer sequence element of arr.

## A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:

5. Hyphun\_indicesArray []: It stores the space of plaintext sequence of base4 number are used to separate number from integer sequence.

ENCRYPTION TECHNIQUE FLOW CHART

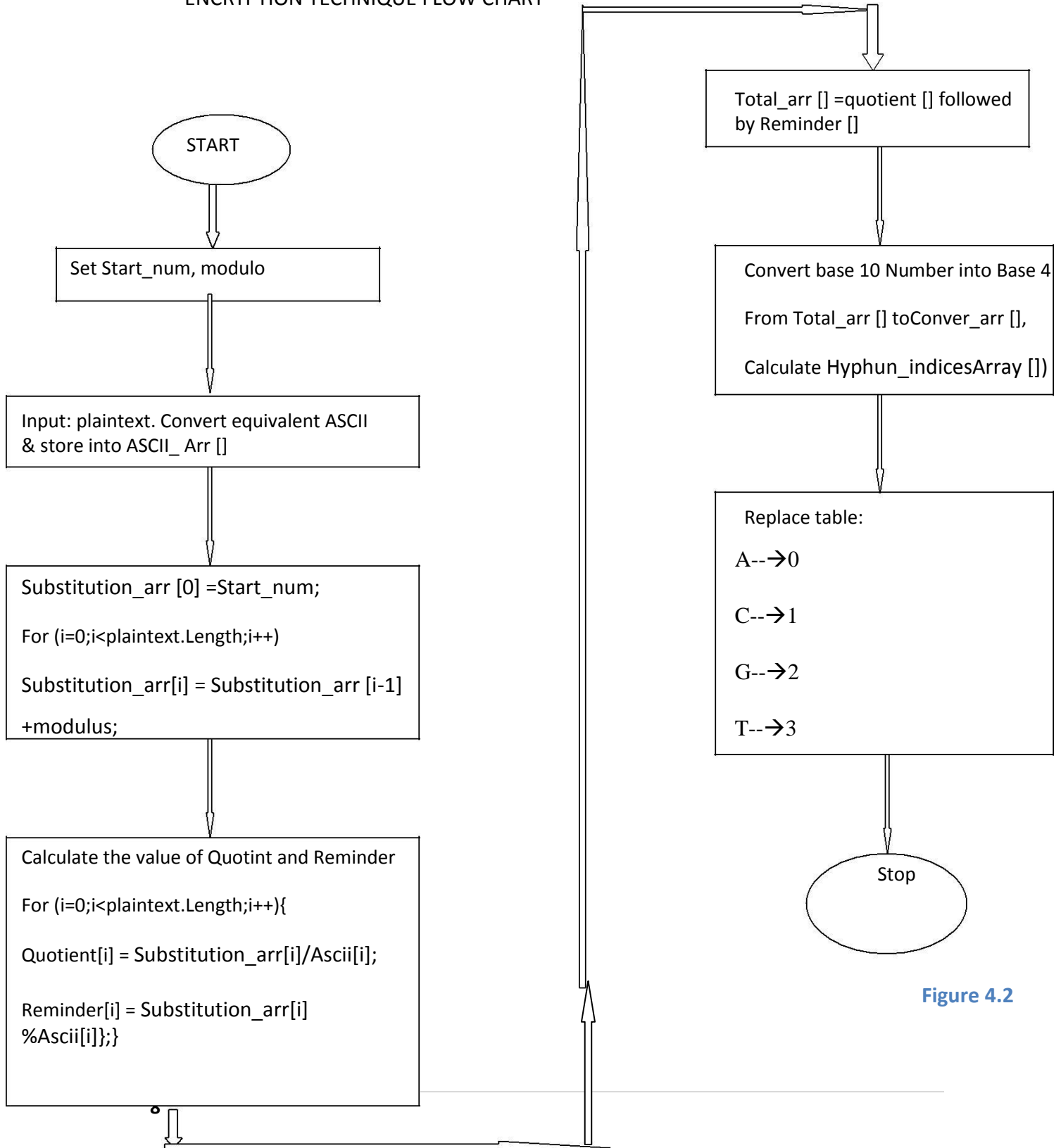


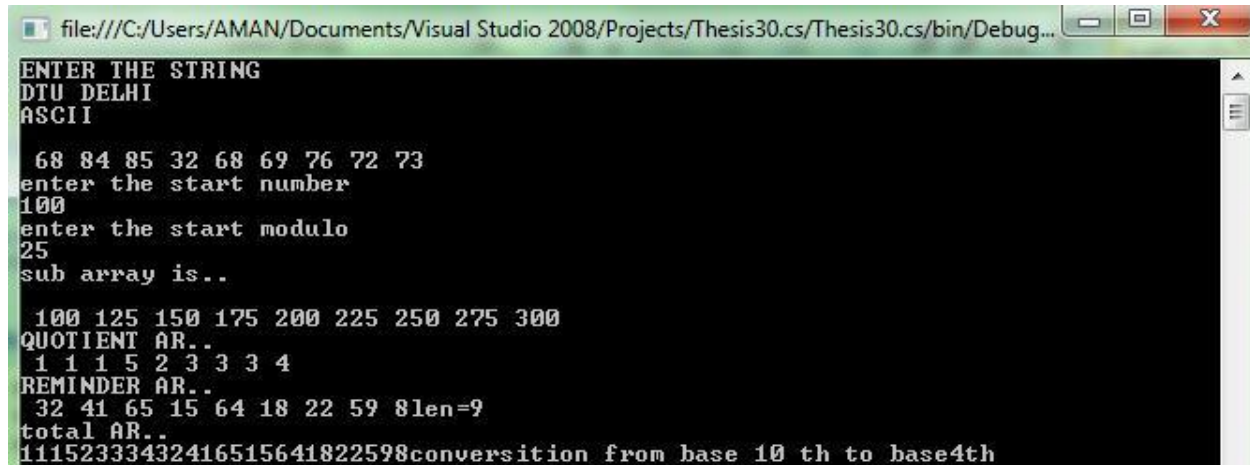
Figure 4.2

## A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:

### OUTPUT OF ENCRYPTION TECHNIQUE:

Plaintext	Ascii[]	Substitution_arr[]	Division	Quotint[]	Reminder[]
D	68	100	100/68	1	32
T	84	125	125/84	1	41
U	85	150	150/85	1	65
''	32	175	175/32	5	15
D	68	200	200/68	2	64
E	69	225	225/69	3	18
L	76	250	250/76	3	22
H	72	275	275/72	3	59
I	73	300	300/73	4	8

Table 5



```
file:///C:/Users/AMAN/Documents/Visual Studio 2008/Projects/Thesis30.cs/Thesis30.cs/bin/Debug...
ENTER THE STRING
DTU DELHI
ASCII
 68 84 85 32 68 69 76 72 73
enter the start number
100
enter the start modulo
25
sub array is..
 100 125 150 175 200 225 250 275 300
QUOTIENT AR..
 1 1 1 5 2 3 3 3 4
REMINDER AR..
 32 41 65 15 64 18 22 59 8len=9
total AR..
11152333432416515641822598conversion from base 10 th to base4th
```

Input Figure 1

## A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:

```
File:///C:/Users/AMAIN/Documents/visual studio 2008/Projects/Thesis30.cs/Thesis30.cs/bin/Debug...
conversion from base 10 th to base4th
sd=3
1
1
1
1
11
2
3
3
3
10
200
221
1001
33
1000
102
112
323
20
hyphun are
2
4
6
9
11
13
15
17
20
24
28
33
36
41
45
49
53
toatal le38
totalcount38
substring array is
11111233310200221100133100010211232320
cipher text is
substring array is
TTTTTCGGGTACAACTTAATGGTAAATACTTCGCGCA
pre of decipher
substring array is
11111233310200221100133100010211232320str=11111233310200221100133100010211232320
1 1 1 11 2 3 3 3 10 200 221 1001 33 1000 102 112 323 20count55
```

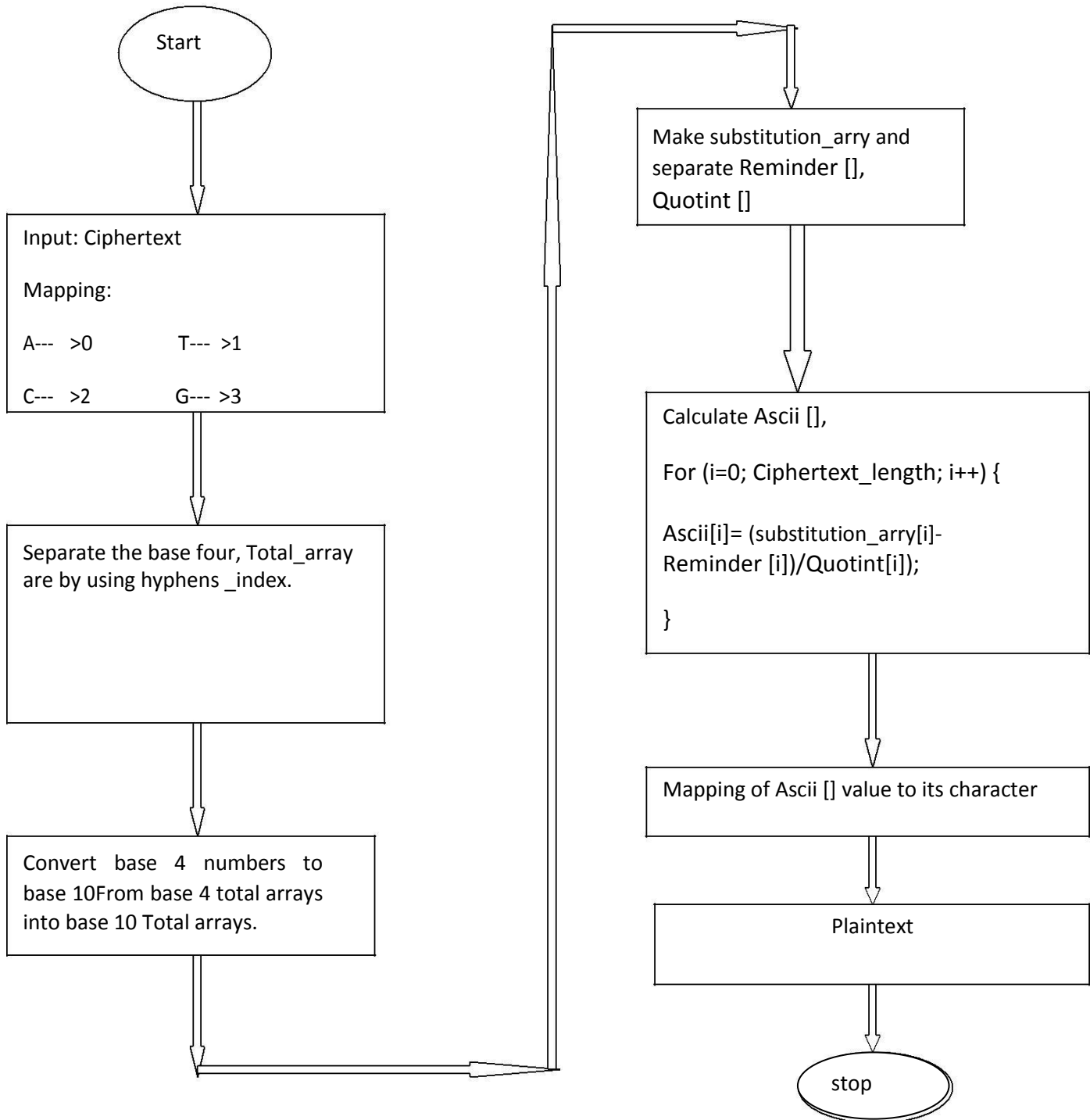
Input Figure 2

**Decryption:**

**Cipher is:**

```
substring array is
TTTTTCGGGTACAACTTAATGGTAAATACTTCGCGCA
```

**FLOW CHART OF DECRYPTION TECHNIQUE:**



## A NOVEL METHOD FOR MAINTAINING SECURITY ON CLOUD COMPUTING:

### OUTPUT OF DECRYPTION TECHNIQU

Quotint[]	Reminder[]	Ascii[]	Substitution_arr[]	Mapping ASCII	Character
1	32	68	100	$(100-32)/1=68$	D
1	41	84	125	$(125-41)/1=84$	T
1	65	85	150	$(150-65)/1=85$	U
5	15	32	175	$(175-15)/5=32$	
2	64	68	200	$(200-64)/2=68$	D
3	18	69	225	$(225-18)/3=69$	E
3	22	76	250	$(250-22)/3=76$	L
3	59	72	275	$(275-59)/3=72$	H
4	8	73	300	$(300-8)/4=73$	I

```
file:///C:/Users/AMAN/Documents/Visual Studio 2008/Projects/Thesis30.cs/Thesis30.cs/bin/Debug...
TTTTTCGGGTACAACTTAATGGTAAATACTTCGGCGCA
pre of decipher
substring array is
11111233310200221100133100010211232320str=11111233310200221100133100010211232320
1 1 1 11 2 3 3 3 10 200 221 1001 33 1000 102 112 323 20count55
bin57
cop..57
num1
num1
num1
num5
num2
num3
num3
num3
num4
num32
num41
num65
num15
num64
num18
num22
num59
num8
subs9
bin=1
bin=1
bin=1
bin=5
bin=2
bin=3
bin=3
bin=3
bin=4
bin=32
bin=41
bin=65
bin=15
bin=64
bin=18
bin=22
bin=59
bin=8
quotient
1 1 1 5 2 3 3 3 4
Reminder 32 41 65 15 64 18 22 59 8
DTU DELHI
substring array is
11111233310200221100133100010211232320
```

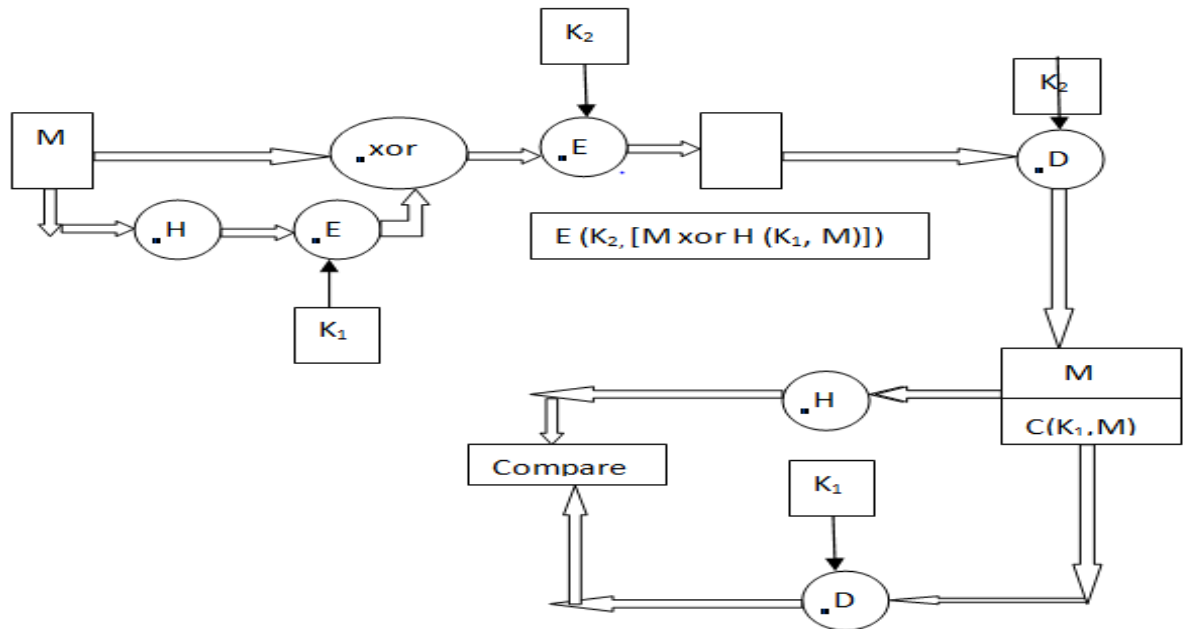
# CHAPTER 5

## Conclusion and Future Work

### CONCLUSION:

Encryption and decryption of all ASCII character are possible. Confidentiality is ensured successfully. It takes less time to any other cryptography algorithm. Therefore availability gets increased and number of users will be increase. DNA has no complex mathematical operation so does not take more computational time as that of other cryptography. DNA is providing both symmetric and asymmetric algorithm. Here symmetric form of DNA has been implemented. It is easy to implement but gives very complex cipher which is almost difficult to break. Since DNA is very new technology to security field so there can be possibility to explore then DNA in future. To provide security here algorithm choose three symmetric key and mapping references. But there is some limitation it can't provide authentication. It can't capture any modification of data.

### FUTURE WORK:



Future work is to be providing authentication property through digital signature. There should have added special function to detect when any modification is taken place in cipher text.

## REFERENCES:

1. Alkady, Y., Habib, M. I., & Rizk, R. Y. (2013). A new security protocol using hybrid cryptography algorithms. *2013 9th International Computer Engineering Conference (ICENCO)*, 109–115. <http://doi.org/10.1109/ICENCO.2013.6736485>
2. Barker, E. B., Barker, W. C., & Lee, A. (2005). Guideline for Implementing Cryptography in the Federal Government. *NIST Special Publication, 800-21*(September 2005), 21. [http://doi.org/NIST Special Publication 800-21](http://doi.org/NIST%20Special%20Publication%20800-21) [Second Edition]
3. Garg, P., & Sharma, V. (2014). Efficient and secure data storage in Mobile Cloud Computing through RSA and Hash function. *2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, 334–339. <http://doi.org/10.1109/ICICT.2014.6781303>
4. Huang, X., Liu, J., Tang, S., Xiang, Y., Liang, K., Xu, L., & Zhou, J. (2014). Cost-Effective Authentic and Anonymous Data Sharing with Forward Security. *IEEE Transactions on Computers, PP(99)*, 1–1. <http://doi.org/10.1109/TC.2014.2315619>
5. It, I. (2014). Deployment of Application on Cloud and Enhanced Data Security in Cloud Computing using ECC Algorithm, (978), 1667–1671.
6. Kalpana, P., & Singaraju, S. (2012). Data security in cloud computing using RSA algorithm. *Ijrcct, 1(4)*, 143–146. Retrieved from <http://ijrcct.org/index.php/ojs/article/view/53>
7. Khanezaei, N. (2014). A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services, (December), 12–14.
8. Liu, H., Ning, H., Xiong, Q., & Yang, L. (2014). Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing. *IEEE Transactions on Parallel and Distributed Systems, 9219(c)*, 1–1. <http://doi.org/10.1109/TPDS.2014.2308218>
9. Mohamed, E. (2012). Enhanced data security model for cloud computing. *Informatics and Systems (INFOS), 2012 8th International Conference*, 12–17. Retrieved from [http://ieeexplore.ieee.org/xpls/abs\\_all.jsp?arnumber=6236556](http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6236556)
10. Mohamed, E. (2012). Enhanced data security model for cloud computing. *Informatics and Systems (INFOS), 2012 8th International Conference*, 12–17. Retrieved from [http://ieeexplore.ieee.org/xpls/abs\\_all.jsp?arnumber=6236556](http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6236556)



11. Paul, M., Collberg, C., & Bamberger, D. (2015). A Possible Solution for Privacy Preserving Cloud Data Storage. *2015 IEEE International Conference on Cloud Engineering*, 397–403. <http://doi.org/10.1109/IC2E.2015.103>
  
12. Pimm, S. L. (2000). Biodiversity is us. *Oikos*, 90(1), 3–6. <http://doi.org/10.1034/j.1600-0706.2000.900101.x>
  
13. Liu Yongliang, Wen Gao, Hongxun Yao, and Xinghua Yu , "Elliptic Curve Cryptography Based Wireless Authentication Protocol," International
  
14. G. Singh, Supriya, "A Study of encryption algorithms (RSA, DES, 3DES and AES) for Information Security," *International Journal of Computer Applications*, vol. 67, no. 19, pp. 33-38, April 2013 *Journal of Network Security*, Vol. A, No. 1, PP. 99-106, Jan. 2007.
  
15. M. J. Dubal, T. R. Mahesh, and P. A. Ghosh, "Design of a new security protocol using hybrid cryptography architecture," In *Proceedings of 3rd International Conference on Electronics Computer Technology (ICECT)*, vol. 5, 2011.
  
16. Subedari Mithila, P. Pradeep Kumar, "Data Security through Confidentiality in Cloud Computing Environment", Subedari Mithila et al, / (IJCSIT) *International Journal of Computer Science and Information Technologies*, Vol. 2 , 1836-1840, 2011.
  
17. DNA Alphabet. VSNS BioComputing Division, <http://www.techfak.uni-bielefeld.de/bcd/Curric/PrwAli/node7.html#SECTION00071000000000000000>, (2011)
  
18. Amin, S. T., Saeb, M., El-Gindi, S., A DNA-based Implementation of YAEA Encryption Algorithm, *IASTED International Conference on Computational Intelligence*, San Francisco, pp.120-125, (2006) Vaida, M.F., Terec, R., Tornea, O., Chiorean, L., Vanea, A., DNA Alternative Security, *Advances in Intelligent Systems and Technologies Proceedings ECIT2010 – 6<sup>th</sup> European Conference on Intelligent Systems and Technologies*, Iasi, Romania, October 07-09, pp. 1-4, (2010)
  
19. Vaida, M.F., Terec, R., Alboaie, L., Alternative DNA Security using BioJava, *DICTAP2011, Conference SDIWC, Univ. de Bourgogne, Dijon, France, 21-23 June, 2011*, pp.455-469
  
20. Java Cryptography Architecture. Sun Microsystems. <http://java.sun.com/j2se/1.4.2/docs/guide/security/CryptoSpec.html> (2011)

