

METHOD TO MAINTAIN DATA SECURITY IN 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:

DHEERAJ AGGARWAL

(2K14/ISY/20)

Under the guidance of

Dr. N. S. RAGHAVA

Associate Professor



Department of Computer Science and Engineering

Delhi Technological University

Bawana Road, Delhi-110042

2013-2015

CERTIFICATE

This is to certify that the thesis entitled “**METHOD TO MAINTAIN DATA SECURITY IN CLOUD COMPUTING**” submitted by **DHEERAJ AGGARWAL(2K14/ISY/20)** to the Delhi Technological University, for the award of the degree of Master of Technology is a bona-fide record of research work carried out by him under my supervision. The contents of this thesis, in full or in part, have not been submitted to any other Institute or University for the award of any degree or diploma.

Place: DTU, Delhi

Date: _____

Dr. N.S Raghava

Associate Professor

Department of ECE

Delhi Technological University,

Delhi.

ACKNOWLEDGEMENT

First I would like to express my gratitude towards my supervisor **Dr. N. S. Raghava**, *Associate Professor, Department of ECE* 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.

DHEERAJ AGGARWAL

Roll No.: 2K14/ISY/20

Dept. of CSE

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 the given method we hide the MAC address using the DNA cryptography. The cryptography technique uses the key obtained by DNA technique; the image is shuffled and then encrypted with the key. The encrypted image is kept at server side and whenever the user wants to access the data he uses the dna key for the decryption.

CONTENTS

CERTIFICATE	2
ACKNOWLEDGEMENT	3
ABSTRACT	4
CONTENTS.....	5
LIST OF FIGURES	7
CHAPTER 1	8
1.1 Introduction	8
1.2 Challenges And Motivation:	9
1.3 Objectives And Contributions	9
CHAPTER 2	11
CLOUD COMPUTING.....	11
2.1 Introduction	11
2.2 Components Cloud Computing	13
2.3 Cloud Evolution	14
2.4 Cloud Computing Architecture	16
2.5 Software As Services	16
2.6 Platform As Service	17
2.7 Infrastructure As A Service (Iaas).....	18
2.8 Cloud Deployment Model	18
2.9 Technical Characteristics	20
2.10 Virtualization And Cloud Computing	22
2.11 Issues In Cloud Computing	24
CHAPTER 3	26
NETWORK SECURITY	26

3.1 Introduction	26
3.2 Security Goals	27
3.3 Threat To Confidentiality.....	28
3.4 Attack Threatening To Integrity.....	28
CHAPTER 4	30
DNA CRYPTOGRAPHY	30
4.1 Introduction	30
4.2 Dna Cryptography	30
CHAPTER 5	36
PROPOSED METHODOLOGY	36
5.1 Introduction	36
5.2 key generation method	37
5.3 Shuffling Of Pixel Based Upon Number Of Successive Iterations.....	37
5.4Encryption of The Shuffled Image Using The Dna Encryption.....	40
5.5 Authentication Of User	42
5.6 Decryption Of Encrypted Image.....	42
CHAPTER 6	44
EXPERIMENTAL SETUP AND RESULTS	44
6.1 Introduction	44
6.2 The Conversion of Mac Address to Dna Sequence.....	44
6.2 Encryption And Decryption Of The Image.....	46
CHAPTER 7	47
7.1 Conclusion.....	47
7.2 Future Work	47
REFERENCES	48

LIST OF FIGURES

Figure 1:Components of Cloud.....	13
Figure 2: Emergence of Various Related Technologies during Different Year	15
Figure 3:DNA Nucleotide Base	31
Figure 4:Structure Of Purines and Pyrimidnes	32
Figure 5:Series of codon in mRNA molecule.....	33
Figure 6:Dna Base Coding.....	37
Figure 7:Padding Of Image.....	38
Figure 8: Position of pixel in shuffled image after 1st iteration	39
Figure 9: Position of pixel in shuffled image after 2nd iteration.....	39
Figure 10:Encryption with Byte Sequence	40
Figure 11:key obtained using DNA Cryptography 1	44
Figure 12:key obtained using DNA Cryptography 2.....	45
Figure 13:Initial Image	46
Figure 14:Encrypted Image.....	46

CHAPTER 1

1.1 Introduction

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. 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 results 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 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 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 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. 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 is provided to cloud user, may be this data can be scattered to other VM.

1.3 OBJECTIVES AND CONTRIBUTIONS

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.

CHAPTER 2

CLOUD COMPUTING

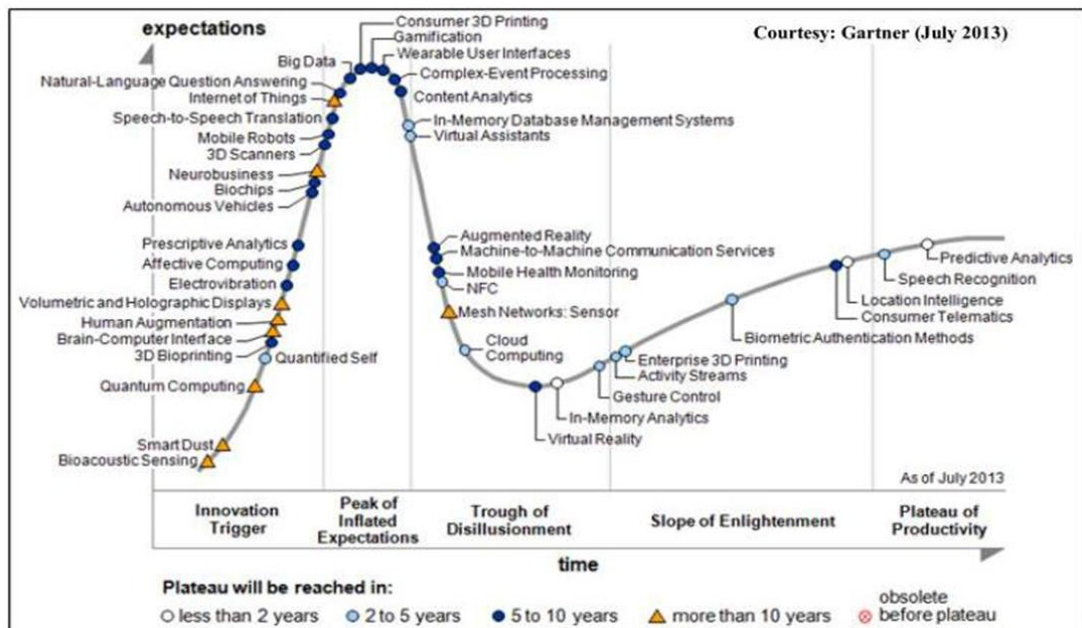
2.1 Introduction

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.

Cloud Computing Definition

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*” Courtesy: Patrick D. Gallagher



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 “**Cloudonomics**” has given by Joe Weinman which defines cloud computing economical perspective, which is discussed below:

1. **Common Infrastructure:** it is a common and standard resource pool that is made available to all the cloud users.
2. **Location 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. **Online connectivity:** There is need of maintain consistent connection via internet to access the services or resource over the cloud.
4. **Utility Pricing:** pay-per-use pricing and benefits the as per their demand.

5. **On-Demand Resources:** Scalable elastic resources are provisioned and de-provisioned without delay or costs associated with change.

2.2 Components 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 1.

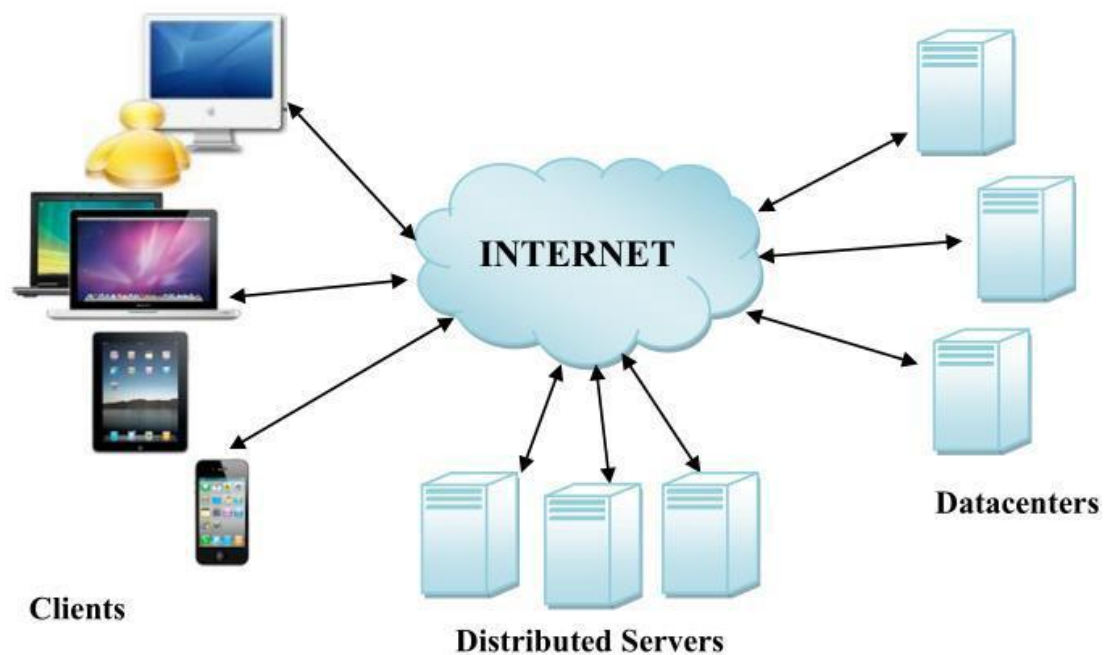


Figure 1: Components of Cloud

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 these components is defined below

Clients

Clients are computers which are used in our day to day works but it may be a laptop, a mobile phone or a tablet computer. But all these clients should be 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.

Datacenters

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

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.

2.3 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.

Brief History

This complete collection is allocate 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 a 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 hard-disk, chunk of memory and one OS the VPN (virtual private network) which offers cheaper and better quality services.

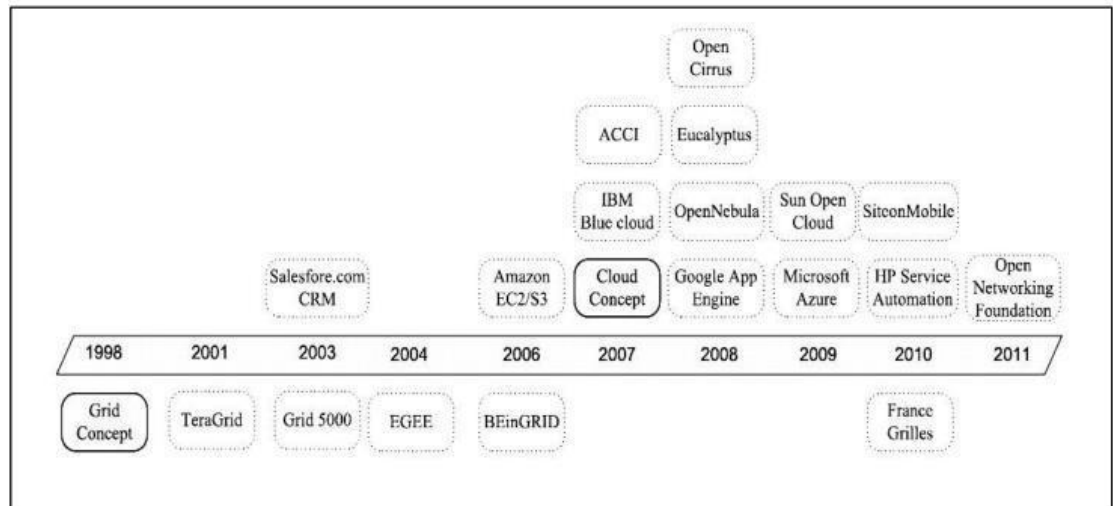


Figure 2: Emergence of Various Related Technologies during Different Year

Comparison 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 autonomic computing.

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.

2.4 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.

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

2.5 SOFTWARE AS SERVICES

Software as service (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 have 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.

2.6 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
- Server side subscription environment

Some popular PaaS service provider companies are Microsoft Azure, Engine Yard and Google App Engine.

2.7 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 own application. Means here clients have not worried about infrastructure as a basic network device, processing power and hardware to develop the application. So in IaaS, clients have own developer, network administrator which is only responsible for configuration of network. A user can deploy and can run any operating system like Linux, Solaris and other software like MATLAB, Code Block, Eclipse, NetBeans etc. User is free from the hurdle of managing the cloud infrastructure which was required to run their application. But has to manage the storage, operating system and deployed 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.

2.8 Cloud Deployment Model

There are numbers of cloud users who want 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 want different size of infrastructure based on services listed by cloud. It defines the services and its boundary.

These deployments are as follow:

Private 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, Google App-engine and many more. On the basis of deployment of cloud, private clouds are divided into two parts

- **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.

- **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.

Hp-cloud start and eBay are 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

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.

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.

2.9 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.

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.

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.

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.

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.

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.

2.10 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.

Key Characteristics of Virtualization:

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

- **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.

- **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.

- **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.

Virtualization Techniques

There are two main virtualization technologies in cloud.

- **Full Virtualization**

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

- **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.

2.11 ISSUES IN CLOUD COMPUTING

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

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.

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.

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 users.

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 of 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.

CHAPTER 3

NETWORK SECURITY

3.1 INTRODUCTION

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 thought 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. An 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.

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.

3.2 SECURITY GOALS

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

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.

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.

Availability

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 except only server should come for managed user's data. There should communication between cloud user and cloud server

3.3 THREAT TO CONFIDENTIALITY

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

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.

Traffic Analysis

Information can be made no intelligible for interceptor by using encrypt text 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

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

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 a 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.

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 id 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.

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 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.

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.

CHAPTER 4

DNA CRYPTOGRAPHY

4.1 Introduction

The science of DNA sequencing deals with identifying the precise order of nucleotides bases within a DNA molecule. It comprises of several methods or technology that aims to determine the order of the four bases—adenine, guanine, cytosine, and thymine—in a strand of DNA. In the early 1970s, academic researchers obtained the first DNA sequence based on two dimensional chromatography. The rapid evolution of DNA sequencing and Sequence Alignments methods has greatly accelerated medical and biological research. DNA sequencing has gain popular application in certain area such as medical diagnosis, biotechnology, forensic biology, virology and biological systematic. The ability of DNA to carry massive parallel information has simulated the use of DNA to hide the information and utilizing then for cryptographic purpose. Thus, giving rise to new domain ‘DNA cryptography’ and which is continuously growing with the exploring of DNA computing.

4.2 Dna Cryptography

Since mid 90’s, a lot of research work is going in the field of DNA Computing. Today, the science of DNA computing posses a high level computational ability and have the potentiality to solve huge and complex mathematical problems. The massive parallel nature of DNA and ability to bear the extraordinary information density is a key feature which has been efficiently utilized by the researchers for data hiding purposes and all sort of cryptographic purposes, giving rise to science of DNA Cryptography. DNA cryptography is a new domain of cryptography and continuously growing with the exploring of DNA computing.

Biological Background of DNA

DNA stands for deoxyribonucleic acid which is germ plasma of all lifestyle. It is a biological macromolecule and is made up of nucleotide. Nucleic acids consist of a chain of linked units called nucleotides. Each nucleotide consists of three subunits: a phosphate group and a sugar (ribose in the case of RNA, deoxyribose in DNA) which forms the backbone of the nucleic acid strand, and attached to the sugar is one of a set of nucleobases. These nucleobases are responsible for double helical structure of DNA which participates in base pairing of DNA strands to form higher-level secondary and tertiary structure.

The four nucleotide bases of DNA strand is shown in the table 1 representing the four nucleotide bases of a DNA strand, which is covalently linked to a phosphodiester backbone.

A	Adenine
T	Thymine
G	Guanine
C	Cytosine

Figure 3:DNA Nucleotide Base

Based on the chemical structures as shown if Fig 3, the four nucleotides A, C, G, T can be divided into two classes:

1. Purine $R = \{A, G\}$ and Pyrimidine $Y = \{C, T\}$
2. Amino Group $N = \{A, C\}$ and Keto Group $K = \{G, T\}$.

Besides these, the division can also be made according to their strength of the hydrogen bonds i.e. weak H-bonds $W = \{A, T\}$ and strong H-bonds $S = \{G, C\}$. [8]

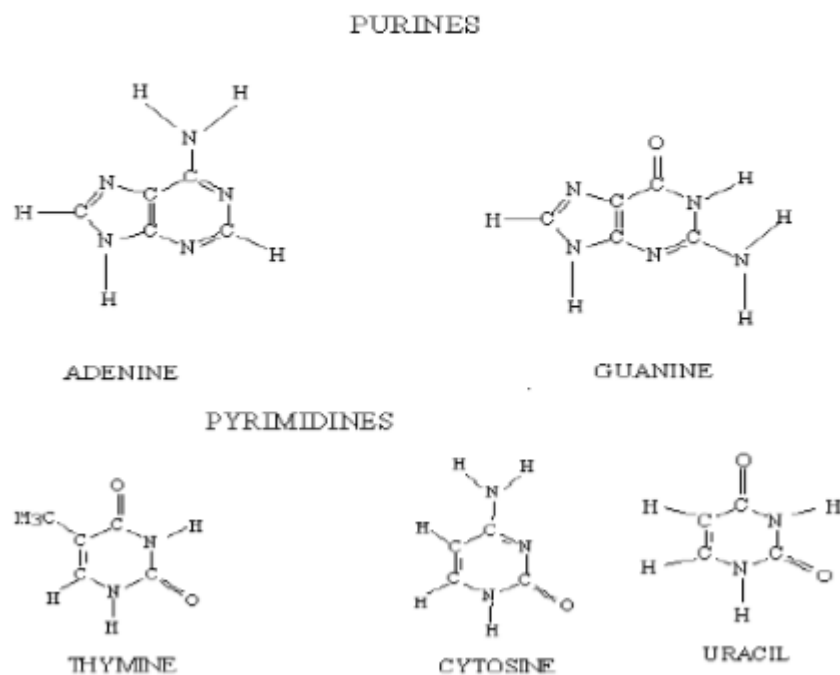


Figure 4: Structure of Purines and Pyrimidines

A gene is DNA sequence which carries the genetic information. Within a gene, a messenger RNA sequence is defined based upon the sequence of bases along a DNA strand. The translation and transcription technique are collectively known as genetic coding. [9][10] It defines the relationship between the nucleotide sequences of genes and the amino-acid sequences of proteins. The genetic code consists of three-letter 'words' called codons composed from a sequence of three nucleotides bases (e.g. ACT, CAG, TTT). In transcription, a DNA segment is transformed into messenger RNA (mRNA) by RNA polymerase, which exits the nucleus and enters into the body of a cell. In translation, the encoded information in mRNA is decoded by ribosome and assembles amino acid into protein chains.

Dna Sequencing

DNA sequencing is the process of determining the precise order of nucleotides within a DNA molecule. Any method or technology that defines the ordering of four nucleotide bases i.e. adenine, guanine, cytosine, and thymine in a DNA strand. The parousia of rapid DNA sequencing methods has greatly accelerated biological and

medical research and discovery. The natural sequence pattern with complementary coding and chemical classification of the nucleotides can be used to shield the message.

One sequence can be complementary to the other sequence, implies that they have the base on each position is the complementary (i.e. A to T, C to G) and in the reverse order. The arrangement of series of codon in a mRNA molecule is shown in Fig 5 describing the complementary properties of nucleotide base. For example, the complementary sequence of ATGC is TACG. Thus, if one is a sense strand then the other is antisense strand and shows complementary behavior to the other strands.

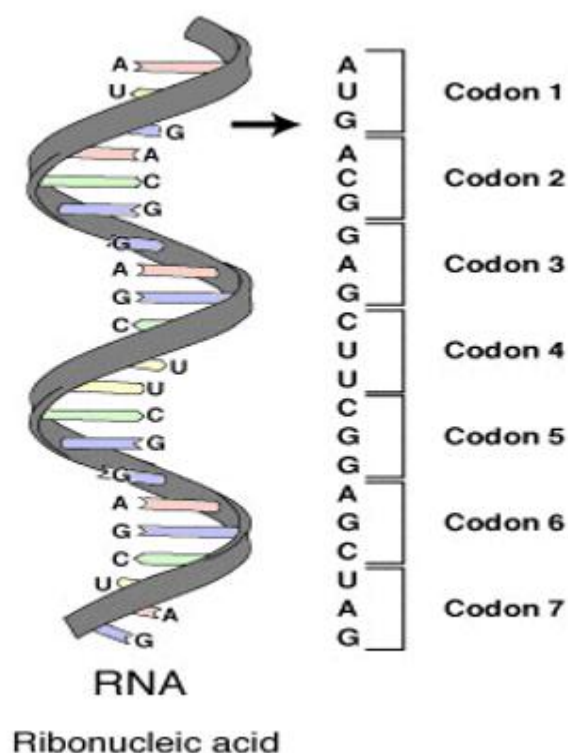


Figure 5: Series of codon in mRNA molecule.

There is one special property for DNA sequences i.e. the real DNA sequence and the faked DNA sequence will almost look like the same. And, there are also a large number of DNA databases which are publicly available. By using these facts, in this paper a new methodology is formed for encrypting messages using DNA sequences.

DNA sequences offer a unique method of encrypting messages or information. The main advantage of DNA sequences is they are composed of letters which are meaningless for most people. The DNA sequence is a combination of A, C, G and T base pairs.

Using these properties of DNA sequences, three complementary rules can be formed and subsequently be used to generate fake DNA sequences. DNA sequence serves as an ultra compact information storage medium which stores a large amount of data in compressed form. A single gram of DNA contains 10^{21} DNA bases = 10^8 tetra bytes.

Thus, these characteristic of DNA:

- Massive parallel computing
- Large data storage
- Information carrier (mRNA)
- Genetic coding
- Generation of faked and random DNA sequences
- Searching complexity of a particular DNA sequence in large database

Has increased the possibility of using DNA and gives a prominent direction in cryptographic research.

There are several DNA-based algorithms that have been practically applied for cryptography purposes. Kang Ning proposes a method in which sender uses the original DNA sequence to encode its secret message and performs transcription and translation obtaining a protein which act as a public key for the receiver. Ning also proves that this cryptography method is secure against many intruder attacks like replay attack, brute force attack though he acknowledges that the encryption complexity increase with key size.

Debnath Bhattacharyya proposed a new data hiding methods based upon DNA complementary rules and message indexing. In this indexing of a random DNA sequence is done which is used as a reference for encoding the message in DNA sequence and during decryption process one requires the DNA string and Index mapping to obtain the original message.

In 2010, H.J. Shiu, K.L. N proposed a more robust method for hiding data. He introduced the insertion method, complementary pair method and substitution method for hiding data in DNA sequence. In the insertion method both the reference DNA sequence and the secret message is decomposed into segments before assembling the segments one by one from the secret message and the reference sequence. In the Complementary Pair Method the complementary rules are used to encode the secret message. In the substitution method, another letter is substituted for an existing letter decided by the algorithm substitution rule.

The DNA-crypt algorithm has also been used for image cryptography. Qiang Zhang, Ling Guo proposed a new scheme of encrypting image using DNA sequences. The proposed approach defines two new mathematical operation on DNA sequences i.e. addition and subtraction operation which helps in combining the encoded matrix block of DNA sequences and then using complementary rules for the output of added matrix block by using chaotic dynamical system(Logistic Map).

Jin-Shiuh Taur et al proposed a method for improving the effectiveness of the substitution method, known as Table Lookup Substitution Method (TLSM), this methods enhance the message hiding capacity twice. In TLSM, the extended the complementary rule definition and introduce a 2-bit rule table instead of 1-bit rule table. Thus, while encoding allowing two bits of secret message to be encoded.

CHAPTER 5

PROPOSED METHODOLOGY

5.1 INTRODUCTION

The proposed encryption and authentication method has been divided into three phases:

Phase 1: KEY GENERATION

Phase2: IMAGE ENCRYPTION USING GENERATED KEY

Phase3: AUNTHENTICATION OF USER

In the proposed scheme, we first start with obtaining the Mac address of the given system and applying DNA cryptography. The obtained key value is shared between two parties and is considered as shared secret key. This key serves as an initialization parameter for proposed encryption algorithm. In the proposed encryption method, the image encryption is done by the Key obtained above and decryption is done using the same key value as a decryption key. The user uploads its encrypted data over the cloud, if any other user wants to access this encrypted data. It needs to be get authorized by the authentication server of the cloud. For authenticating, an authentication approach is proposed in which user authentication is carried out through secure key exchange for validating user legal identities and once the authentication is done successfully, the actual symmetric key is given to user through secured channel, through which it can access the encrypted data over the cloud.

5.2 KEY GENERATION METHOD

Step 1: Obtain the MAC address of the current user system who wants to upload the encrypted data over the cloud. The MAC address obtained is in hexadecimal notation which is converted into binary notation to get 48-bit address.

Step 2: Obtained 48-bit binary address (having MAC address) is converted into DNA sequence strands on the basis of following rule given by table

S.NO	DNA BASE	CODE	S.NO	DNA BASE	CODE
1	AA	0000	9	GA	1000
2	AC	0001	10	GC	1001
3	AG	0010	11	GG	1010
4	AT	0011	12	GT	1011
5	CA	0100	13	TA	1100
6	CC	0101	14	TC	1101
7	CG	0110	15	TG	1110
8	CT	0100	16	TT	1111

Figure 6: Dna Base Coding

This method of hiding data in a random DNA sequence is known as DNA Cryptography. Thus for given input 48-bit message we get a 24-bit DNA Sequences which is the compressed form of the original message.

Example of DNA Cryptography:

Suppose, we have a message $M = '10101001'$, and we need to hide this message in DNA sequence. On the basis of mapping rule specified above we get the corresponding DNA sequence for this given message which is 'GGGC'. Thus, we get a compressed DNA sequence having length 4 just half of the original message.

5.3 Shuffling Of Pixel Based Upon Number Of Successive Iterations

Shuffling helps in changing the correlation among the adjacent pixels. With this transformation the image is being apparently randomized and the original image

is regained after number of back tracking steps. The shuffling of image depends upon the size of the image. It does the shuffling for the image having even number of rows and columns and if the dimension not matched the extra padding with zero matrix is done. Shuffling of pixel is done in two steps:

Step1 For every iteration, a quadrant is sub divided into equal sub-quadrants.

STEP 2 For each t iteration,

if 't' is odd($2n-1$) then the rotation of quadrant is done in anti-clockwise direction.

If 't' is even($2n$) then the rotation of quadrant is done in clockwise direction.

Example:

To padding (Figure 7) and shuffling of pixel(Figure 8,Figure 9) is illustrated with an example given below.

Consider an image, having size $P \times Q$, where $P=4$ and $Q=5$, so total number of pixel in an image is 20. Therefore, it undergoes iterations 3 times, moreover we also see that number of rows $P=4$ which is even but number of columns $Q=5$ is not even and thus padding of zero matrix is done having dimension $[P, 1]$ to the number of columns. The shuffling and padding of image is shown by the Fig 7

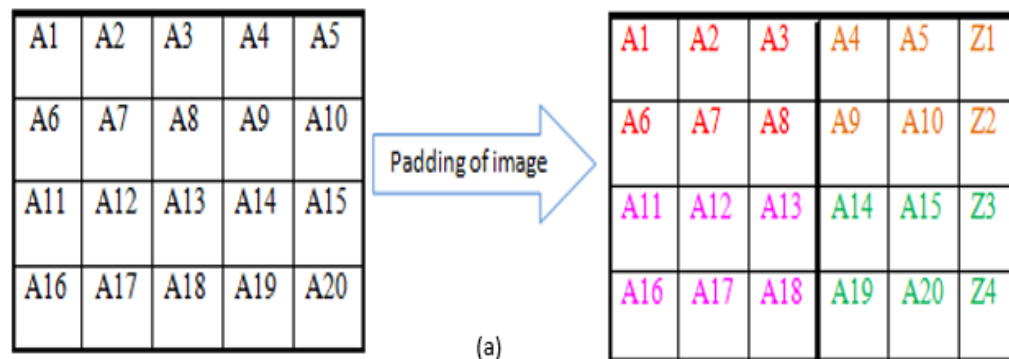
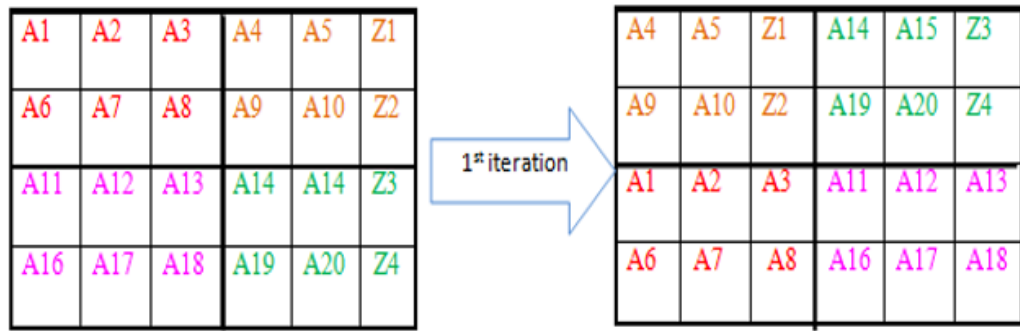


Figure 7: Padding Of Image



(b)

Figure 8: Position of pixel in shuffled image after 1st iteration



Figure 9: Position of pixel in shuffled image after 2nd iteration

5.4 Encryption of The Shuffled Image Using The Dna Encryption

The obtained shuffled image is then encrypted using the key from DNA cryptography.

In this method,

- We first find the binary form of the MAC address.
- This MAC address is mapped to DNA sequence as explained above in the algorithm
- Reduction of obtained sequence is done by combining each consecutive 4-bits and converting them into decimal notation. (figure 10)

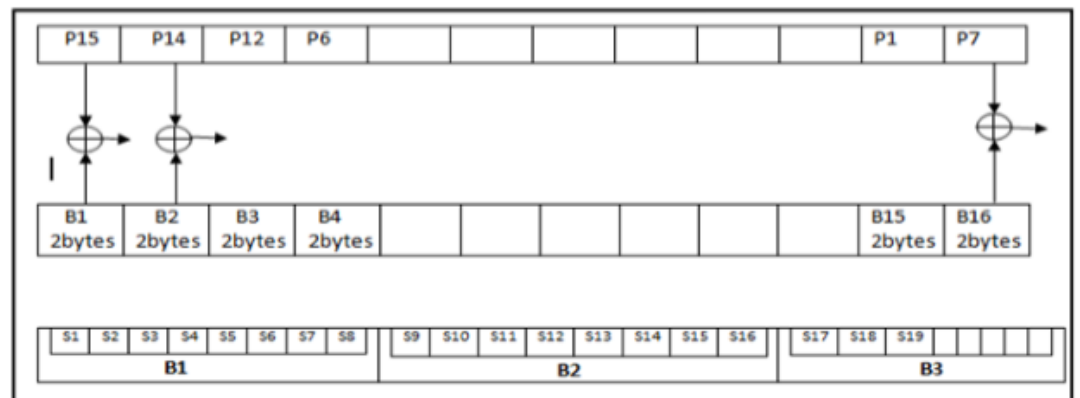
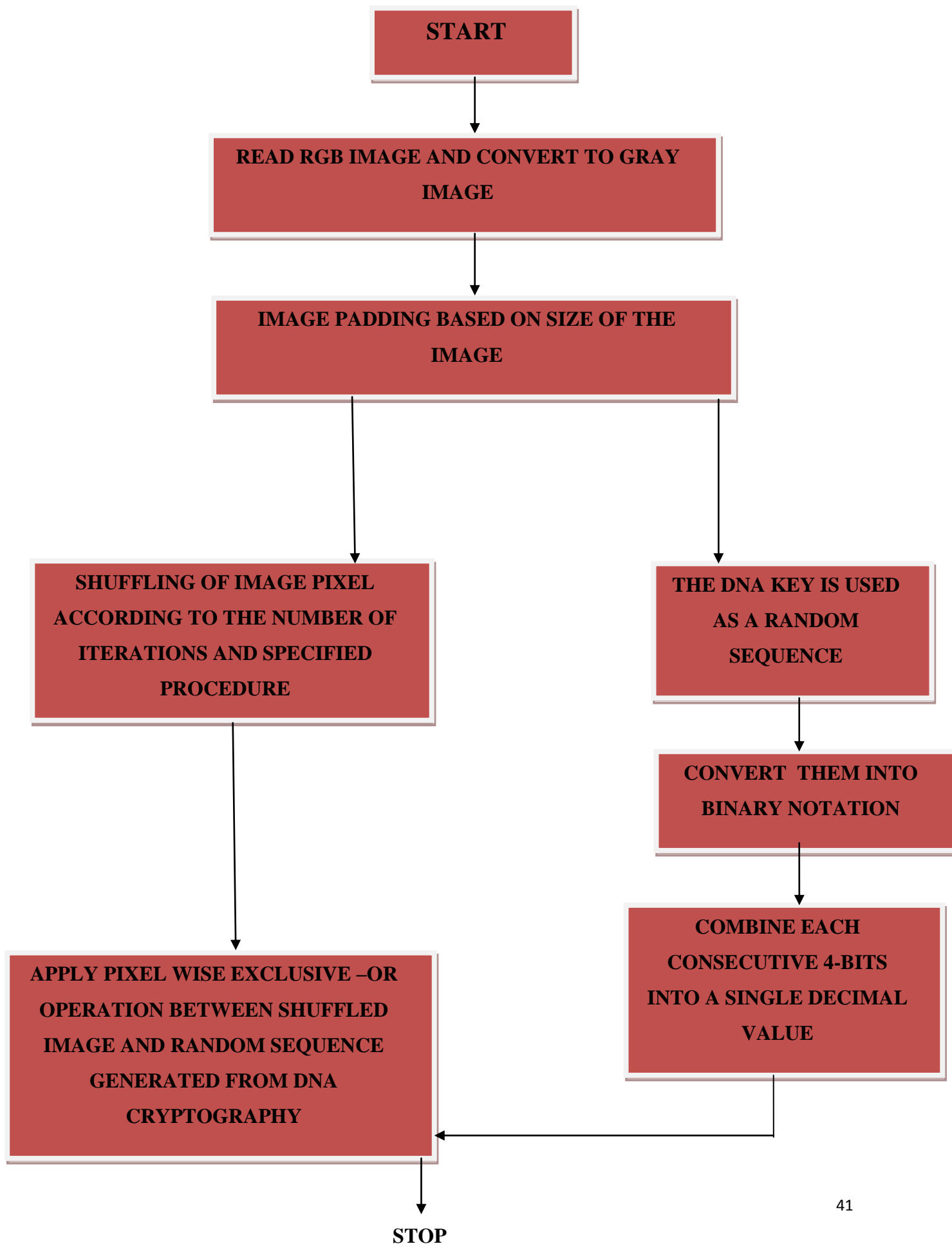


Figure 10: Encryption with Byte Sequence

- This is the final step in which bitwise Exclusive-OR operation is done between the pixel of shuffled image and the sequence generated from the DNA cryptography. Here the confusion is done by the shuffling of pixel on different permutation and then the encryption is applied on the image.

Flow chart of Image Encryption Algorithm



5.5 Authentication Of User

In this phase, we proposed a novel user authentication approach and secure key exchange in order to validate the legitimate identity of user. we proposed to use a modified version of the two-server model in which there are two servers one is authentication server and another is database server. the authentication server is responsible for validating the user request and once the user get authorized it get access to encrypted data stored on database server. The database server stored the encrypted data and list of legitimate user who can access this data. The list consists of mac address of those users to whom the access is granted. The user authentication and encryption steps are explained below:

Suppose, there are two clients user A and user B, authentication server (as) and database server (ds).

User A wants to upload a file (image file .jpeg) on cloud server; it first generates the key dna cryptography mentioned above and encrypts the file using the key as explained above. It also provides the list of legitimate user to authentication server with whom user a wants to share this encrypted file.

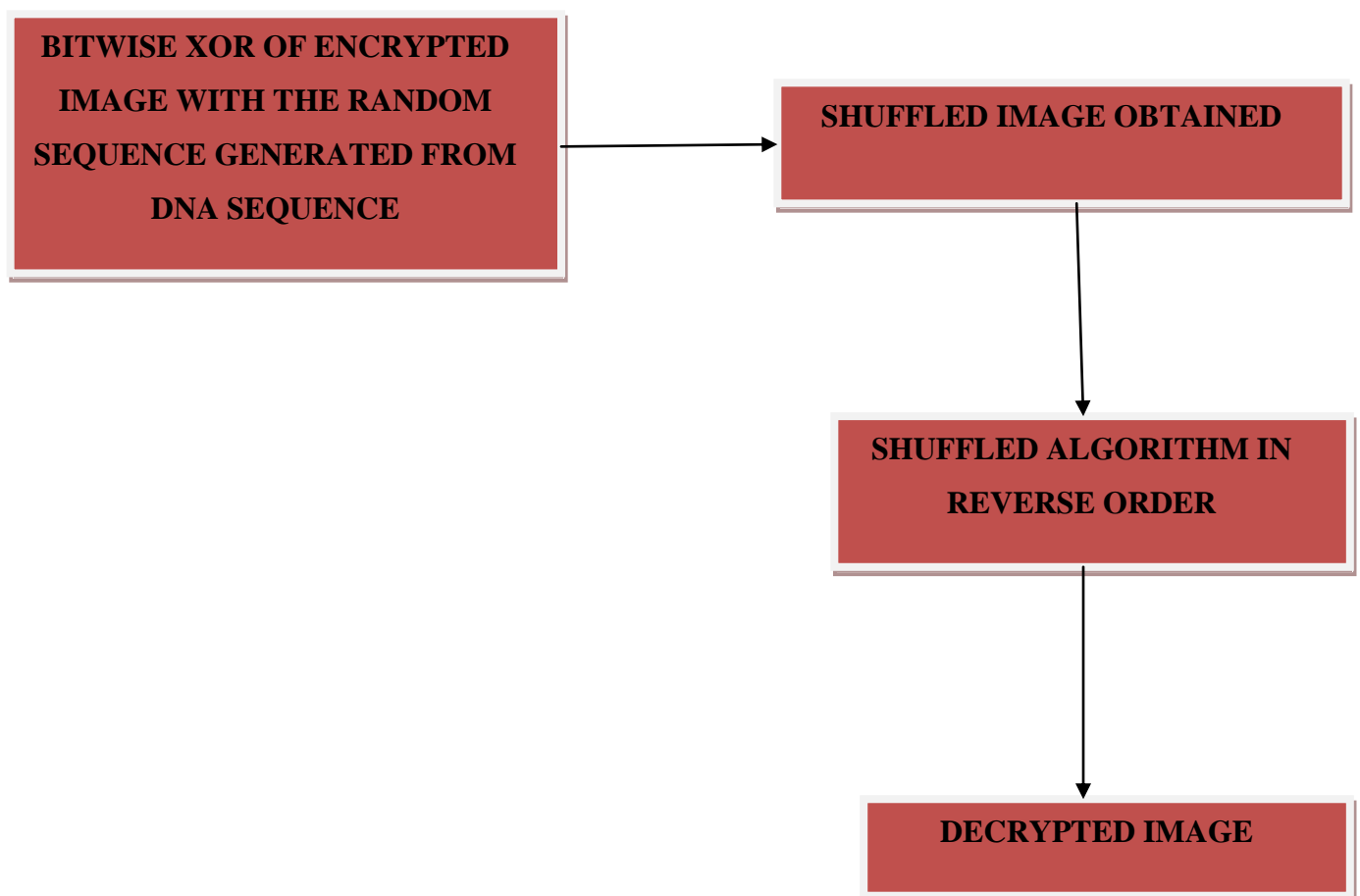
Now, if user B wants to read this file it first needs to be get authorized. The authorization is done on the basis of mac address. If user B mac address matches with the specified mac address in the legitimate user list stored over the authentication server (as), then user b is successfully validated and can get access to the encrypted file stored on database server (ds).

5.6 Decryption Of Encrypted Image

The encrypted image is uploaded on the cloud, along with the authentication details .If the other user wants to decrypt it first needs to get the key i.e. the key found using DNA cryptography . Once, the initialization parameter is obtained, the decryption is done to get the shuffled image. This shuffled image is rearranged in the same order by back tracking the encryption algorithm in order to obtain the original image.

- The key which was found in DNA cryptography is Xor with the encrypted image.
- From the above step we get the shuffled image.
- Using the shift iteration we shift the image and get the original image.

Decryption Flow Chart



CHAPTER 6


EXPERIMENTAL SETUP AND RESULTS

6.1 Introduction

The following system configuration has been used while conducting the experiments:

- Processor: Intel Core i3
- Main Memory: 4 GB
- Hard Disk Capacity: 512 GB
- Software Used: MATLAB R2010a

6.2 The Conversion of Mac Address to Dna Sequence



```
"G:\code block\secure.exe"
ENTER THE MAC ADDRESS
FFFFFFFFFFFF
THE ENTERED MAC ADDRESS IS FFFFFFFFFF
ENCRYPTION START
THE MAC ADDRESS CONVERTED TO BITN 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
DNA ENCRYPTION
TT TT TT TT TT TT TT TT TT TT TT TT
ENCRYPTION ENDS
SEND TO SERVER
DECRYPTION START
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1
F F F F F F F F F F F F
COMAPRE WITH DATABASE
AUTHENICATION PROVIDED TO THE USER
Process returned 34 (0x22)   execution time : 11.253 s
Press any key to continue.
```

Figure 11: key obtained using DNA Cryptography 1

```
"G:\code block\secure.exe"
ENETR THE MAC ADDRESS
12FFA2244678
THE ENTERED MAC ADDRESS IS 12FFA2244678
ENCRYPTION START
THE MAC ADDRESS CONUERTED TO BITN 0 0 0 1 0 0 1 0 1 1 1 1 1 1 1 1 0 1 0 0 0 1
0 0 0 1 0 0 1 0 0 0 1 0 0 0 1 1 0 0 1 1 1 1 0 0 0
DNA ENCRYPTION
AC AG TT TT GG AG AG CA CA CG CT GA
ENCRYPTION ENDS
SEND TO SERVER
DECRYPTION START
0 0 0 1 0 0 1 0 1 1 1 1 1 1 1 1 0 1 0 0 0 1 0 0 0 1 0 0 1 0 0 0 1 0 0 0 1 1 0
0 1 1 1 1 0 0 0
1 2 F F A 2 2 4 4 6 7 8
COMAPRE WITH DATABASE
AUTHENTICATION FAILED
Process returned 21 (0x15)   execution time : 33.794 s
Press any key to continue.
```

Figure 12: key obtained using DNA Cryptography 2

Figure 11 and Figure 12 shows the conversion of mac address to Dna sequence. The mac address is converted to binary form and then mapped to Dna sequence.

6.2 Encryption And Decryption Of The Image



Figure 13: Initial Image

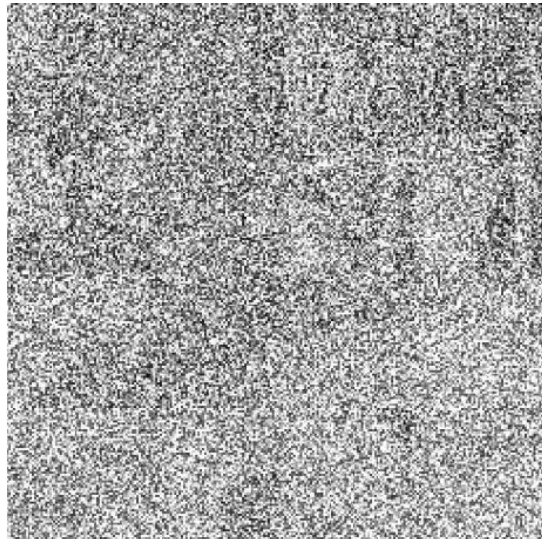


Figure 14: Encrypted Image

Figure 13 shows the initial image, after shuffling of the image and applying the encryption technique we get the encrypted image as shown in figure 14

CHAPTER 7

7.1 Conclusion

This thesis work proposed an efficient cryptographic and authentication framework for cloud computing with many security features such as mutual authentication, secure key exchange, data isolation and data integrity. In this work, three approaches were proposed they are key generation, image encryption using dna sequence, user authentication. The encryption algorithm is based on DNA cryptography which are known for randomness and unpredictable behavior, so it is highly secured. The confusion is enhanced by shuffling of pixel. So, here security is provided at each and every phase. Initially security is provided in the from of authenticated the user so that he can communicate with the server. Next in order to access the data present in the cloud, the data is first encrypted and then stored on the cloud, using the key the user has to decrypt it and can access the data, so it provide privacy of data and other user cannot get to know the original data. Next, if other user has to access the data he also authenticated first and then also he will be provided the access for data. So, at each and every stage of data access various techniques are used which provide complete security of data.

7.2 Future Work

The efficiency of proposed methodology can increased in several aspects like increasing efficiency, and computational complexity and security.

- Generating keys of larger size more than 128-bits and using AES encryption for handling this large key size.
- In this thesis, the proposed encryption technique based on symmetric keys cryptography. This work can be extended to asymmetric cryptography.
- Using asymmetric cryptography techniques, the authentication can also be done using digital signature.
- DNA hybridization technique can be used in key generation phase, to ensure more security and randomness of the seed.(symmetric key)

REFERENCES

- [1] M. Sugumaran, BalaMurugan. B, D. Kamalraj, "An Architecture for Data Security in Cloud Computing", World Congress on Computing and Communication Technologies,2014
- [2]www.networkworld.com/article/2194263/tech-primers/authentication-in-thecloud.html
- [3] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Towards Secure and Dependable Storage Services in CloudComputing," IEEE Transactions on Services Computing, vol.5,no. 2, 2012,pp. 220-232.
- [4] T S Khatri and G B Jethava, "Survey on data Integrity Approaches used in the Cloud Computing, International Journal of Engineering Research & Technology, vol.1, Issue 9, November, 2012.
- [5] Saenger, Wolfram (1984). Principles of Nucleic Acid Structure. New York: SpringerVerlag
- [6] Watson JD, Crick FH (1953). "A Structure for Deoxyribose Nucleic Acid" (PDF). Nature 171 (4356): 737–738.
- [7] Alberts, Bruce; Johnson, Alexander; Lewis, Julian; Raff, Martin; Roberts, Keith; Walters, Peter (2002). Molecular Biology of the Cell; Fourth Edition. New York and London: Garland Science.
- [8] Clausen-Schaumann H, Rief M, Tolksdorf C, Gaub HE (2000). "Mechanical stability of single DNA molecules". Biophys J 78 (4): 1997–2007.
- [9] Crick, Francis (1988). "Chapter 8: The genetic code". What mad pursuit: a personal view of scientific discovery. New York: Basic Books. pp. 89–101
- [10] Kang Ning(2009),"A Psuedo DNA Cryptography Method", Cornell University Library
- [11] Debnath Bhattacharyya, Samir Kumar Bandyopadhyay," Hiding Secret Data in DNA Sequences", International Journal of Scientific & Engineering Research Volume 4(2013)

- [12] Mohammad Reza Abbasy, Bharanidharan Shanmugam, "Enabling Data Hiding for Resource Sharing in Cloud Computing Environments Based on DNA Sequences", IEEE 2011
- [13] L. M. Pecora and T. L. Carroll, "Synchronization in Chaotic Systems", *Physical Review Letters*, vol. 64, no. 8, pp. 821–824, 1990
- [14] *Sync: The Emerging Science of Spontaneous Order*, Steven Strogatz, Hyperion, New York, 2003, pages 189-190.
- [15] [Lorenz, Edward N. (1963). "Deterministic non-periodic flow". *Journal of the Atmospheric Sciences* 20 (2): 130–141
- [16] G. Jakimoski and L. Kocarev, "Analysis of recently proposed chaos –based encryption algorithm", *Physics Letter A*, 2001.
- [17] Wang, Xingyuan; Zhao, Jianfeng (2012). "An improved key agreement protocol based on chaos". *Commun. Nonlinear Sci. Numer. Simul.* 15 (12): 4052–4057.
- [18] Babaei, Majid (2013). "A novel text and image encryption method based on chaos theory and DNA computing". *Natural Computing, an International Journal* 12 (1): 101–107.
- [19] Wikipedia Chaos theory: Definition of chaos at Wiktionary;
- [20] Hasselblatt, Boris; Anatole Katok (2003). *A First Course in Dynamics: With a Panorama of Recent Developments*. Cambridge University Press
- [21] Alligood K.T, T.D Sauer, J.A Yorke, "Chaos an Intoduction to Dynamical systems", First ed 1996, New York: Springer-Verlag
- [22] Bertuglia C.S and F.Vaio, "Nonlinearity, Chaos & Complexity The Dynamics of Natural and Social Systems", First ed. 2005, United States: Oxford University Press Inc
- [23] Werndl, Charlotte (2009). "Are Deterministic Descriptions and Indeterministic Descriptions Observationally Equivalent?". *Studies in History and Philosophy of Modern Physics* 40 (3): 232–242.
- [24] M. S. Baptista, "Cryptography with Chaos", *Phys. Lett. A*, vol. 240, 1998.

- [25] R. Schmitz and J. Franklin, "Use of Chaotic Dynamical Systems in Cryptography", vol. 338, 2001
- [26] Kotulski Z, Szczepariski J. Discrete chaotic cryptography (DCC). In: Proc NEEDS 97
- [27] Shiguo Lian, Jinsheng Sun, Zhiquan Wang(), "A block cipher based on a suitable use of the chaotic standard map", Science direct (2004)
- [28] FIPS PUB 180-1, "Secure Hash Standard", Federal Information Processing Standard(FIPS), Publication 180 -1, National Institute of Standards and Technology, US Department of Commerce, Washington D.C., 1995.
- [29] Lu HP, Wang SH, Hu G. Pseudo-random number generator based on coupled map lattices. Int J Modern Phys B 2004;18(17–19): 2409–14
- [30] Sh. Li, X. Mou and Y. Cai, "Pseudo-Random Bit Generator Based on Couple Chaotic Systems and its Applications in Stream-Cipher Cryptography", INDOCRYPT 2001, LNCS, Springer-Verlag, Berlin, 2001
- [31] Whitfield Diffie, Martin E Hellaman, "New Directions In Cryptography", IEEE Transactions On Information Theory, Vol.It-22, No.6, November 1976.
- [32] H. J. Shiu, K. L. Ng, J. F. Fang, R. C. T. Lee and C. H. Huang, "Data hiding methods based upon DNA sequences", Information of Science, vol.180, no.11, pp.2196-2208, 2010.
- [33] D.Erdmann and S.murphy,"HENON STREAM CIPHER",Electronics Letters,23rd april 1992 vol.28 no.9
- [34] Zeng X.,R.A Pielke and R. Eykholt, "Chaos theory and its application to the Atmosphere",Bulletin of the American Meteorological Society,1993.74(4):p.631-639
- [35] Claude E. Shannon, "Communication Theory of Secrecy Systems", Bell System Technical Journal, vol. 28-4, page 656–715, 1949.
- [36] Wikipedia source, "https://wiki/Confusion_and_diffusion",
- [37] Qiang Zhang *, Ling Guo, Xianglian Xue, Xiaopeng Wei,"An Image Encryption Algorithm Based on DNA Sequence Addition Operation",Key Laboratory of Advanced Design and Intelligent Computing ,2011

