

# An Encryption of Data in Cloud Using BDEA Cryptography and Model View Controller

**B.sivasankari**

Computer Science and Engineering Department, Apollo Engineering College  
Chennai, TamilNadu  
sivashankaripitam@gmail.com

**Abstract**—Cloud computing is the important paradigm of IT industry which deploy distributed computing pattern. It serves as online and on demand storage, services on network, platform as services and so on. Providing secure data transmission is one of the major issues and so most of the organizations are uninvolved in using the series provided by the cloud server. In order to discourse this issue, there have been applied numerous proposals by various researchers, worldwide to render tight security to the data stored in the cloud. The existing encryption technique focuses on the ASCII code, and only can encrypt files in windows application.. Thus the proposed work comprises of enhancement in the BDEA (Bi-directional DNA Encryption Algorithm) to use with Unicode character and MVC technique to encrypt files that user want to upload in the cloud.

**Keywords**-- Cloud computing, Data security issues, Bi-Directional DNA Encryption Algorithm, DNA digital code, Model View Controller

## I. INTRODUCTION

The concept of cloud computing has emerged from cluster, grid, and utility based computing. Cluster and grid computing takes maximum advantage on using many computers in parallel to solve problems of any size. Utility services and software services provides computing advantages and dynamic resources as a service with the notion of pay for what we use. The cloud computing enables us to access services from anywhere, at anytime which is convenient and on demand network access from a shared pool of customizable computing resources (example: networks, servers, storage, applications and services) that can be rapidly deployed and managed. Cloud computing is leverageable to dynamic resources to deliver large number of services to the end users. It is of high throughput computing (HTC) paradigm whereby the infrastructure as a service provider services through a large data farm or server farms. The cloud computing model enables users to share access to resources from anywhere at any time through their connected device. All computation in cloud applications are distributed to servers in data center.

The deployment models of cloud has 4 models and they are private, public, hybrid, community. Public cloud is laid over Internet and it is accessible to any user who has subscribed for the service. Private cloud is raised within the domain of an private network access owned by a single organization. Hybrid cloud is composed of both public and private clouds.

There were three different cloud service model based on pay for what you use band services. And they are Infrastructure as a service model allows user to make use of virtualized IT resources for computing resources, storage and networking.

Software as a service model is a software application that is used to access information across World Wide Web for millions of cloud customers. Platform as a service model involves in developing, deploying and managing the execution of computing request from user by provisioning resources. Many capable security issues may occur in a cloud environment, if suppose qualified security techniques are not been placed. Computational clouds are initiated by the aim to share processing resources among many organizations to bring solution for large-scale problems.

First, a user job is to demands for the resource site to ensure security by providing a security demand (SD). In contrarily, the resource site needs to open its trustworthiness, called its trust index (TI). These two parameters must be satisfied. When enhancing its security demand, users may think about some typical attributes. The entities have to choose other entities which can meet up the requirements of trustworthy to work with that. The entities that submit requests to the resource providers should trust that they will try to process their requests and returns the results with a specified QoS. In order to provide the proper trust relationship between cloud entities, two criteria must be followed. One is to authenticate and the other authorize entities, for all this proper login system of the users should be ensured. The privacy and data security in cloud is achieved through some algorithms that use encryption of data in the cloud. One such encryption is now applied only to encrypt messages. The ASCII character message is converted using this encryption technique and the generated message is ready to send. And this encryptions only available in windows application. No support is provided for the user in this encryption in any other fields. In the proposed work the system can encrypt files that user want to upload in cloud using model view controller as a web application.

## II PROPOSED SYSTEM

In this proposed system we can upload all type of files that user want to encrypt. Here we need not want to encrypt the files separately and upload; the files will be encrypted during the upload itself. The preliminary idea is to make the user less work on uploading the encrypted file. The uploading file is first converted to bytes and then the DNA digital coding applied to it. The encrypted file is automatically stored as a string in the database.

### A. *Authentication*

In order to encrypt files using this algorithm the user has to register the details in the web application. This module is for getting user information through modernized form. The details of each user registered will be maintained as a database in sql server. After successful registration the user can move to the login page for logging in. the authentication is done using login. Once after logging in, user has to choose the file to get encrypted.

### B. *Encryption process*

The uploaded files will be encrypted while uploading itself. This encryption process is highly secure because it has two encryption for total encryption of file. Firstly the uploaded files are stored in sql server, then these files are converted to bytes. Then the bytes are converted to binary, the binary code are then converted using DNA digital coding. Then the AGTC combination is again converted to binary using key combination. The encrypted file will be saved in text document.

**C. DNA Digital Coding**

The binary digital coding uses by two state 0 or 1 and a combination of 0 and 1 for encoding. DNA encoding uses 4 bases (G, C, T and A). Those units are concrete, discontinuous values. ADENINE(A) and THYMINE(T) or CYTOSINE(C) and GUANINE(G) in DNA sequence. The simplest coding pattern to encode nucleotide bases (A,T,G,C) is by means of four digits: 0(00),1(01),2(10),3(11),there are possibly  $4!=24$  possible pattern by encoding format like (0123/CTAG)

TABLE I  
DNA ENCODING

BINARY VALUE	DNA DIGITAL CODING
00	A
01	T
10	G
11	C

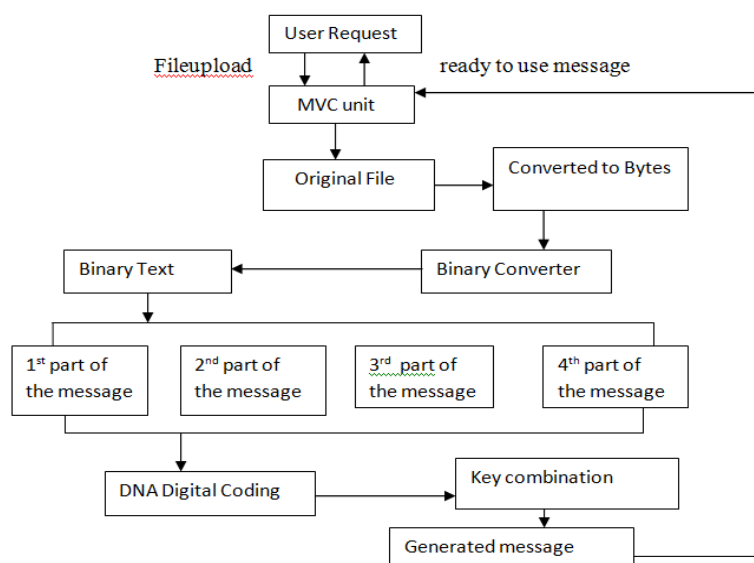
TABLE II  
KEY COMBINATIONS

KEY COMBINATION	PATTERNS	VALUES
AA	0101	5
AT	0011	3
AG	0001	1
AC	0010	2
TA	0110	6
TT	1111	15
TG	0111	7
TC	1001	9
GA	1010	10
GT	0100	4
GG	1000	8
GC	1100	12
CA	1110	4
CT	1011	11
CG	0000	0
CC	1101	13

**D. Model View Controller.**

The Model-View-Controller is an design pattern in which an application is partitioned into three main logical components: the model,the view, and the controller. These components are used to handle their own specific development access of an application. The model is used for data management of the application. It performs actions to the request from the view and it also acts accordingly to the instructions from the controller to manipulate itself. The view is used for presenting the data in a particular format. The controller functions to the user input and provide interactions on the data model objects.

### III. ARCHITECTURE DIAGRAM



The user uploads the file in MVC unit and that original file is then converted to byte transformation. The converted byte message is again then fed into the binary converter. The binary text is partitioned into four parts. The divided messages are encrypted using DNA Digital coding by using its 16 bit key combinations. Thus the generated message is sent back to the user for further use.

### IV. CONCLUSION

Ensuring Data security is fundamental scope of cloud. Different types of cryptographic algorithms like AES, DES, SHA etc, have been used to achieve security of data that is stored in the cloud. The user can make use of any kind of cloud services. File encryption is done using different algorithms with different disadvantages, centered mainly on amount of data compression. It aims at providing high security at just single click. Web applications makes user easy to encrypt and upload files directly to the cloud using Model view controller and DNA digital coding technique. Thus we get a highly secured, reliable and time saved files.

### REFERENCES

- [1] Prajapati Ashishkumar B, Prajapati Barkha: "Implementation of DNA cryptography in cloud computing and using socket programming" 2016 International Conference on Communication System and Network Technologies (IEEE Computer Society)..
- [2] PrashantRewagad, YogitaPavar, "Use of Digital Signature with Diffie-Hellman Key Exchange and AES
- [3] Encryption Algorithm to Enhance Data Security in Cloud Computing" 2013 International Conference on Communication System and Network Technologies (IEEE Computer Society).
- [4] Tusbar Mande, Vijay Choudhary. "A DNA encryption technique based on matrix manipulation and secure key generation scheme". Information Communication and Embedded Systems (ICICES), International Conference on 21-22 Feb 2013.
- [5] Olga Tornea, and Monica E. Borda, "Security and complexity of a DNA-based cipher," IEEE Roedunet International Conference (RoEduNet), 11th, pp. 1-5, 2013
- [6] Ashish Prajapati, Amit Rathod "Enhancing security in cloud computing using Bi-Directional DNA Encryption Algorithm", International Conference on Intelligent Computing, Communication & Devices. (ICCD-2014), Springer.