

---

## **DATA SECURITY USING DISTRIBUTED AND PARALLEL SYSTEM WITH DUAL ENCRYPTION**

**Mr.Naveen TH<sup>\*1</sup>, Anand BY<sup>\*2</sup>, Pavan L<sup>\*3</sup>, Maheshwari SN<sup>\*4</sup>, Rakshitha RK<sup>\*5</sup>**

<sup>\*1</sup>Assistant Professor, Department Of Computer Science And Engineering, Government Engineering College, Krishnarajapet, India.

<sup>\*2,3,4,5</sup>UG Scholar, Department Of Computer Science And Engineering, Government Engineering College, Krishnarajapet, India.

DOI : <https://www.doi.org/10.56726/IRJMETS37833>

---

### **ABSTRACT**

Cloud-based totally data storage carrier has drawn growing pastimes from every academic and organisation in the contemporary years due to its green and low-rate control. since it offers offerings in an open network, its miles pressing for provider vendors to utilize secure data storage and sharing mechanism to ensure data confidentiality and carrier purchaser privateness. To shield touchy data from being compromised, the most broadly used technique is encryption. however, really encrypting facts (e.g., via AES) can't simply deal with the practical want of statistics manages. besides, an effective access manipulate over down load request moreover desires to be taken into consideration so that financial Denial of Sustainability (Edo's) attacks cannot be launched to restriction customers from playing carrier. on this paper, we consider the twin get right of entry to govern, in the context of cloud-based garage, inside the revel in that we design a manipulate mechanism over each records access and down load request without lack of safety and overall performance. two twin get admission to manipulate systems are designed on this paper, wherein each of them is for a distinct designed putting. the safety and experimental evaluation for the structures are also provided.

**Keywords:** Cloud-Based Data Sharing, Access Control, Cloud Storage, Intel SGX, Attribute-Based Encryption.

---

### **I. INTRODUCTION**

Cloud computing is a generation this is primarily based on resource sharing, which aims to provide cohesiveness and economies of scale. This technology offers numerous advantages, but it is not immune to security risks and issues. in this regard, this study targets to recommend a realistic method to privateness and protection troubles with the cloud. One way to increase statistics availability and safety is by dividing data into smaller chunks the usage of herbal genetic code and mystery records tactics. the ones DNA encrypted facts fragments can then be allotted among several cloud company carriers (CSPs) to make certain at ease statistics storage and transmission. The large boom in facts period, from gigabytes to petabytes, is because of the emergence of a huge amount of actual records within the contemporary era. Cloud compute provide data offering, and end result, attackers and complicate users try to unauthorized get right of entry to private cloud. To combat this, the sector of DNA-primarily based information encryption targets to improve statistics security. This paper offers an revolutionary DNA-based facts encryption approach for the pc community, that's rooted in the organic concept of DNA. Them a chine generates a secret key the usage of a decimal encode rule, an America preferred Code for data Interchange values, DNA molecules bases, and a complimentary rule, which makes it able to protecting itself against various protection threats. The proposed method is more efficient and effective than existing methods, as shown by theoretical analysis and actual results To combat this, the field of DNA-based data encryption aims to improve data security. This provides an new DNA-based information encrypt approach for the computer network, which is rooted inside the biological concept of DNA. The system generating a key using a decimal rule, an Standard Code Interchange (ASCII) , DNA molecules base, and a complimentary rule, which makes it capable of protect itself against different heats.

### **II. RELATED WORK**

One of the approaches is the use of multi-clouds, which involves distributing data across multiple cloud service providers to reduce the risk of data breaches and improve data availability.

DNA-based statistics encryption is every other method that has received interest in current years. DNA cryptography makes use of the herbal residences of DNA, consisting of its complex structure and the 4 base pairs, to carry out encryption and decryption. Numerous study have demonstrate effective of DNA cryptography in secure static transmission, storage. In addition to multi-clouds and DNA cryptography, other methods, such as homomorphic encryption, attribute-based encryption, and secure computation, have also been proposed to address the security challenges of cloud computing. Homomorphic encryption allows for data processing on encrypted data, while attribute-based encryption enables data access control based on attributes of users. Secure computation enables multiple parties to perform computations on shared data without revealing the data to each other. Overall, method have show promise result in address the security challenge cloud computing. However, there is still a need for further research to improve the efficiency and effectiveness of these techniques in practice. The proposed DNA-based data encryption method aims to address some of the limitations of existing methods and provide a practical solution to privacy and security issues in the cloud.

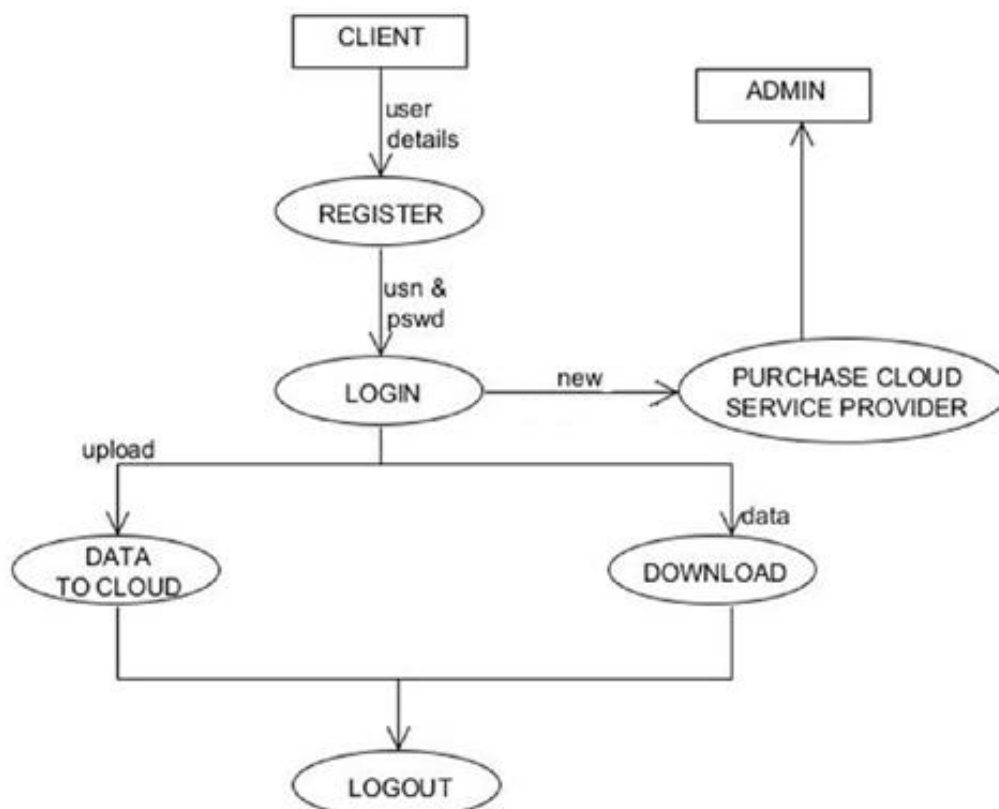
### III. PRESENT SYSTEM

Although cloud compute has many advantages, there are number of secure risk and difficult. Utilizing a "single cloud" provider seems to be less popular due to the likelihood of these dangers, including severe, a Multimedia Access Control (MAC) address, user attributes, and DNA computing are used to generate a 1024-bit mystery key interruption, data theft, data leaking, and the potential for malicious insider assault. A practical solution to this issue is the use of several clouds, sometimes called as "number of co," "inter-clouds," or "cloud cover of clouds."

### IV. PROPOSED SYSTEM

Important consumer statistics can be divided into smaller chunks, with some thrilling functions of natural DNA's nucleotide order and hiding utilized records principles to growth availability of facts and protection. The DNA-encrypted data fragments will then be made available to providers of cloud services (CSP). Therefore, a viable strategy to security and privateness problems with the cloud is recommended in this paper.

### V. SYSTEM ARCHITECTURE



The cloud computing on a customer in a cloud-base employee. The user add add records to cloud even as maintain privacy. The two facts are shown below.

A. Embedding records:

person facts A = 0011011000110101 must be transformed to Cipher-text the usage of decimal rule, base two rule, new form of A, index of Nucleotides, and cipher text.

DNA reference collection is: DNA reference series is mapped to consumer statistics, which is sent to the cloud as 710713.

B. Record Extracting: this are steps:

- A = Cypher textual content.
- find the reference index of nucleotides
- A = preceding shape of A
- comply with the opposite base pairing policies.
- Get = DNA series.
- Convert A to binary the use of binary coding rule
- Get A= man or woman records

assume private records ssss A = 710713 need to be cloud-primarily based completely downloads. The technique for converting

cipher-text to character information is demonstrated below.

DNA reference series is:

a) AA1 AT2 CC3 CG4 CT5 GA6 CA7 AC8 TT9 GT10 TC11 AG12 GG13 TA14 GC15 TG16

b) A = 710713

c) Sub-Part1 (choosing Indexes from reference collection); A = CA GT CA GG

C. Algorithm006D: DNA cryptography uses revolutionary innovations in conjunction with DNA computation, PCR, and array to encrypt facts. A single DNA gramme has 1021 bases, or 108 terabytes of information.

DNA BASE	BINARY VALUE
A	00
G	01
C	10
T	11

Fig-1: DNA Combination

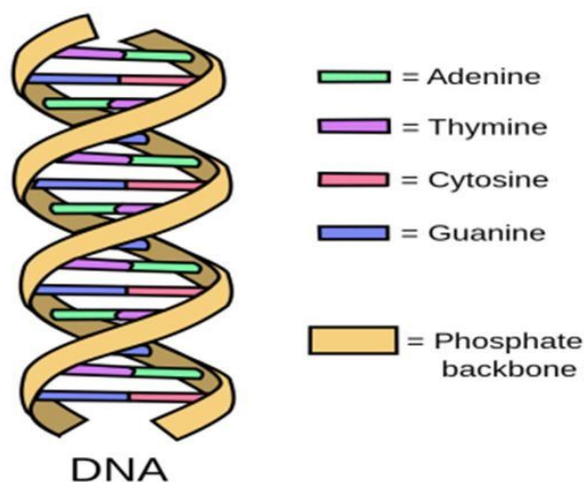


Fig-2: DNA structure

## VI. MODULE DESCRIPTION

### Admin:

**Login:** Admin creates providers by providing valid credentials.

**Manage Cloud:** Manage Multiple clouds from different cloud service providers.

### Client :

**Register:** client get register by giving user details.

**Login:** client will login by giving valid username and password

**Upload:** upload the data to cloud.

**Download:** download the data from cloud

### DNA:

**Splitting of data:** Data is split based on domain.

**DNA Encryption:** The data should be encrypted. The encrypted data should be sent to the cloud service provider.

**DNA decryption:** The data that has been uploaded on the service providers should be combined. Then the combined data should be decrypted before downloading the data.

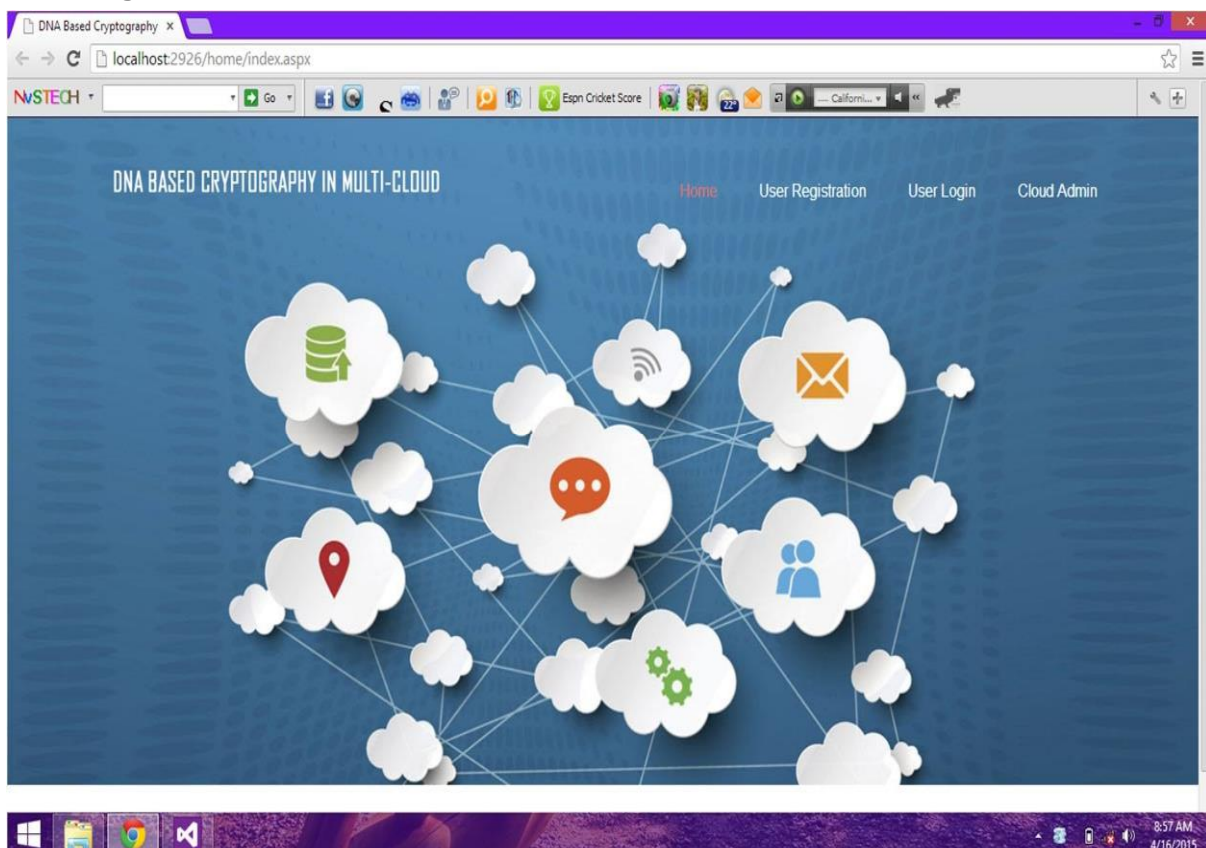
### Rijndael:

Rijndael is an AES algorithm that encrypts and decrypts data by iteration, supporting encryption key sizes of 128, 192, and 256 bits.

## VII. RESULT AND DISCUSSION

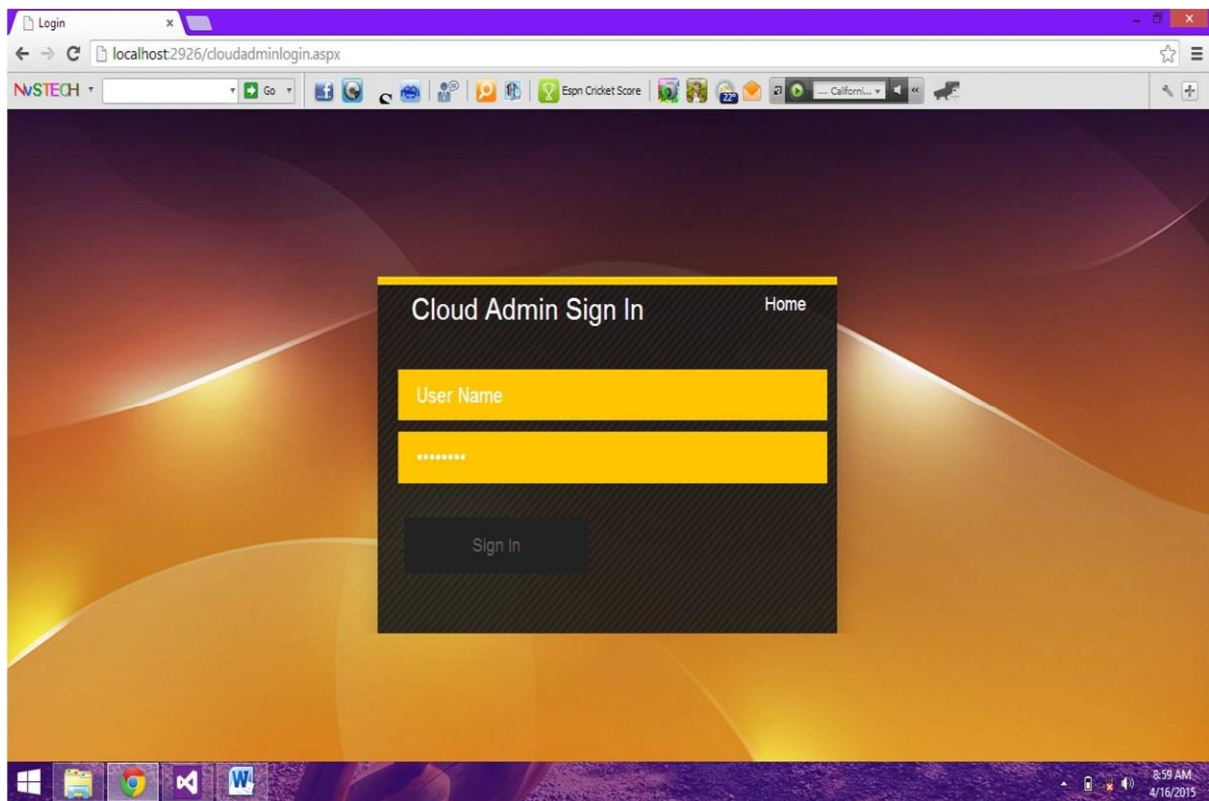
We tested the system by inputting the data to ensure that the algorithm utilized in the system is robust and data is getting slice, encrypted and stored to multi cloud. As predicted, the algorithm sliced the data, encrypted and stored to multi-cloud, while fetching the data sliced data will get joined and decrypted .

### A. Home Page

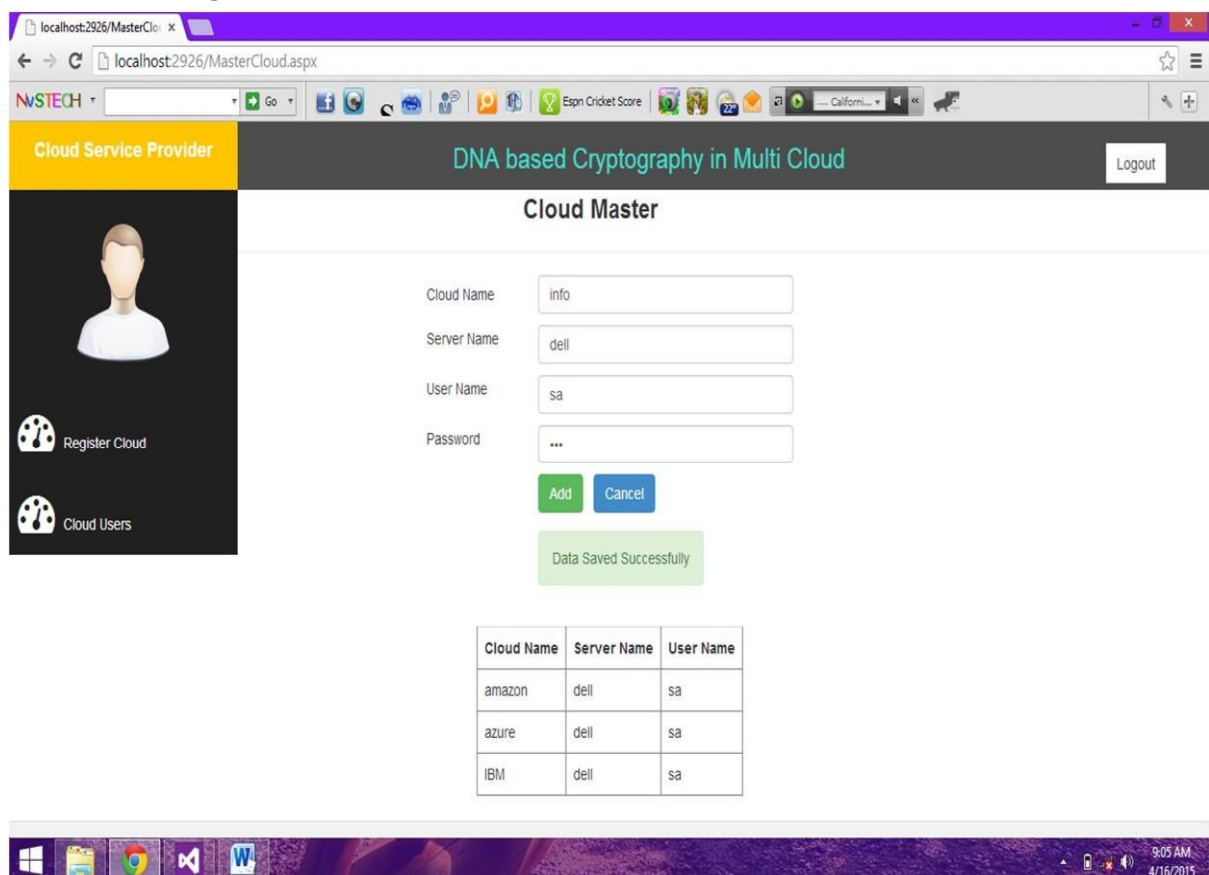




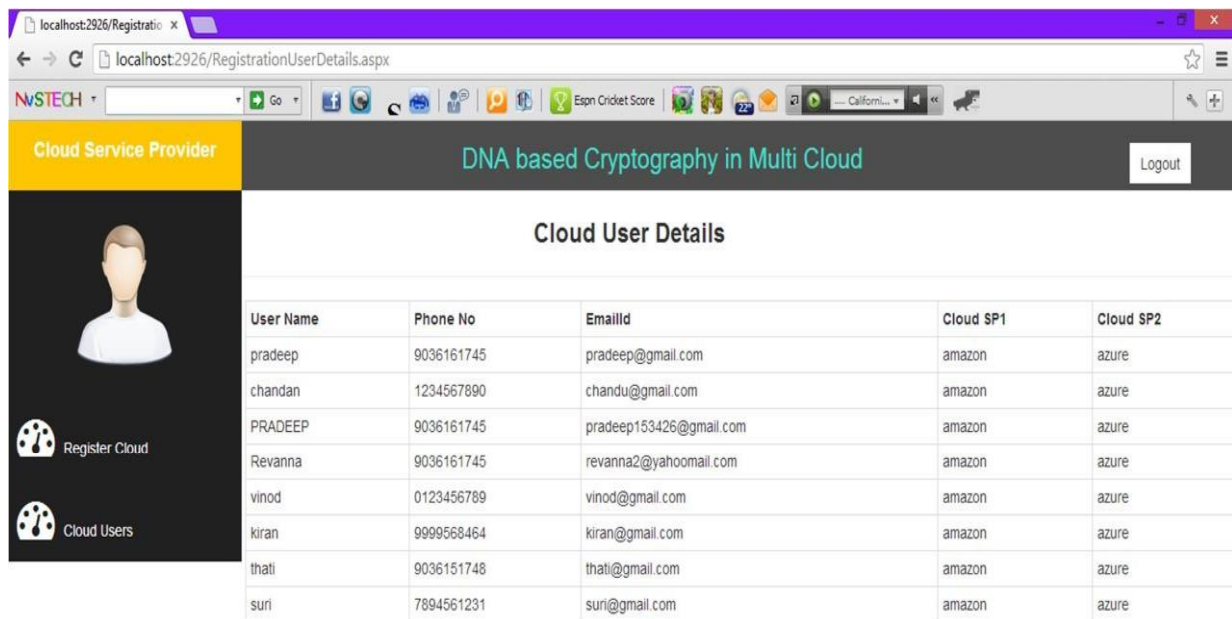
## B. Admin Sign in Page



## C. Admin Home Page and Create Cloud



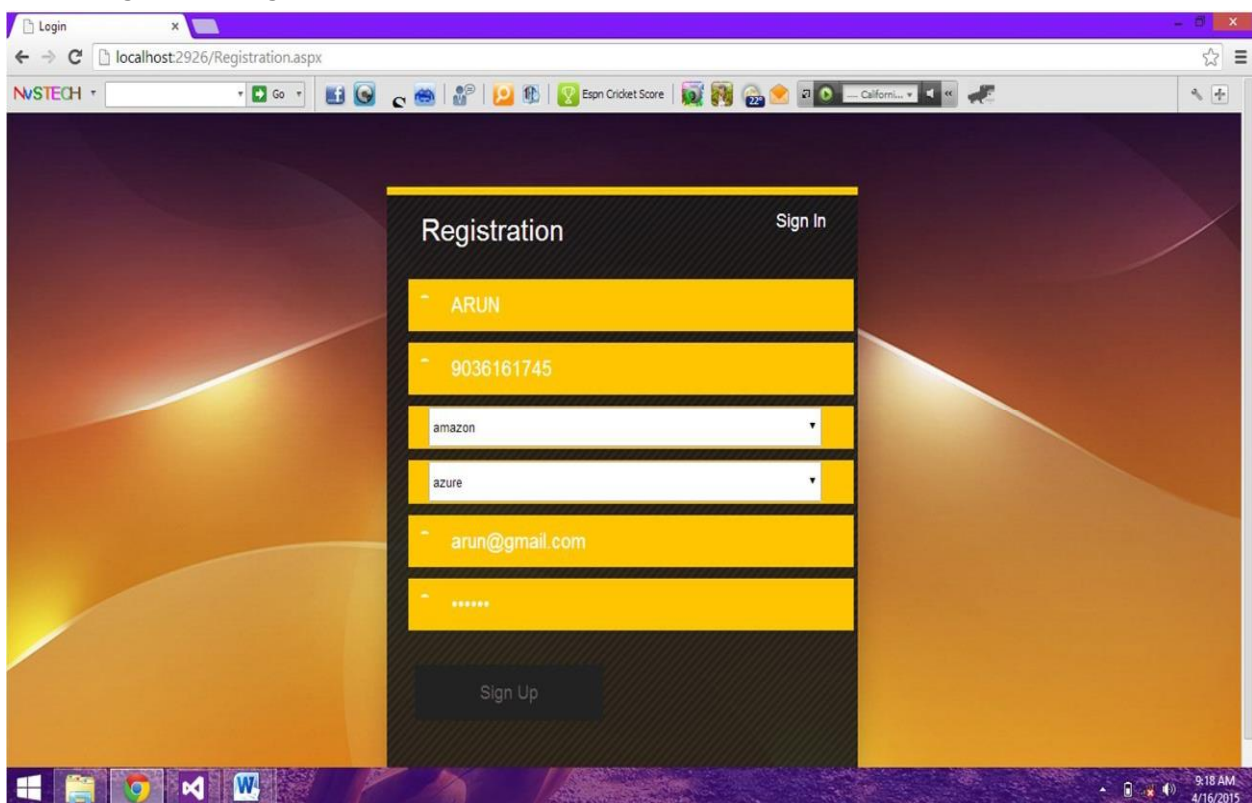
#### D. Admin View the Cloud User



The screenshot shows a web application interface for an administrator. The top navigation bar includes a 'Cloud Service Provider' dropdown, the title 'DNA based Cryptography in Multi Cloud', and a 'Logout' button. The main content area is titled 'Cloud User Details' and displays a table of registered users. On the left sidebar, there are buttons for 'Register Cloud' and 'Cloud Users'.

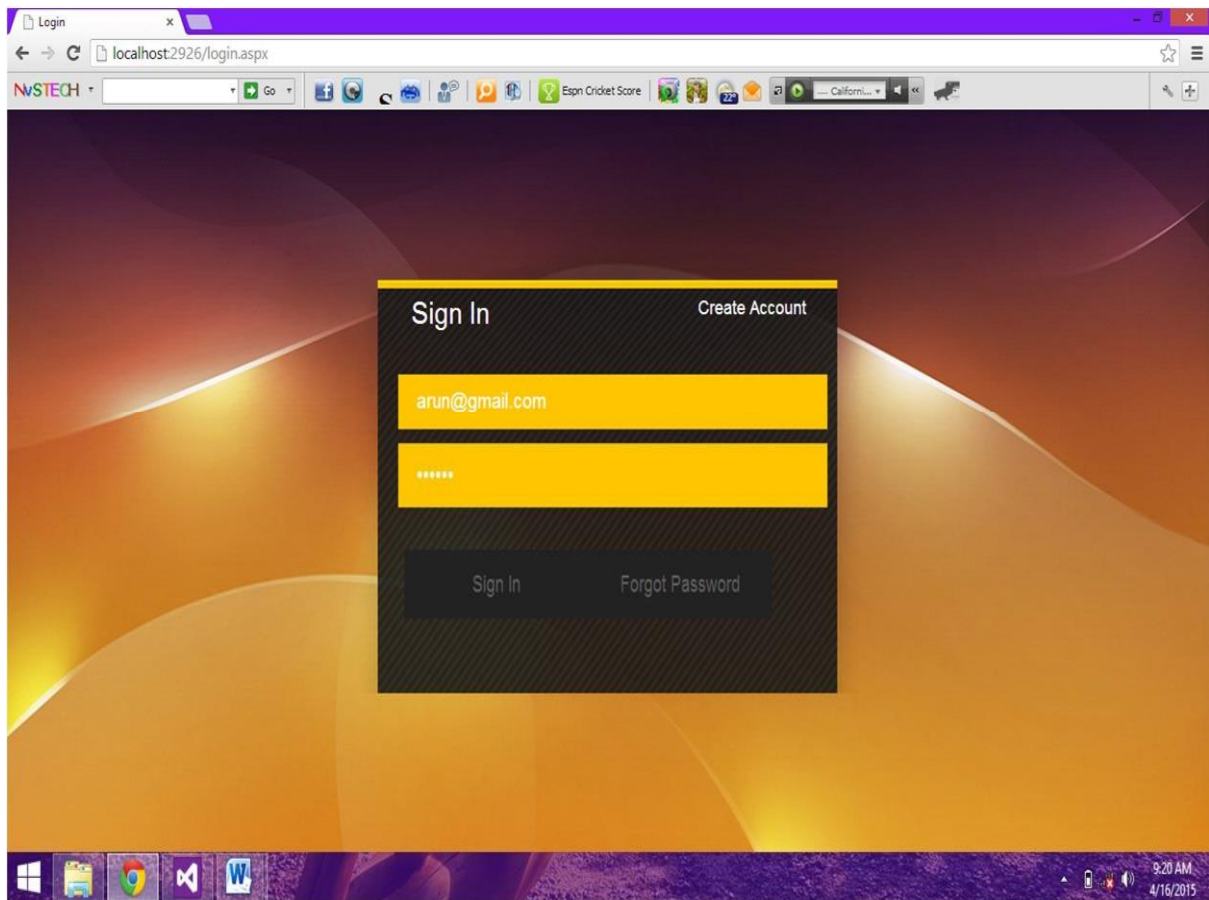
User Name	Phone No	EmailId	Cloud SP1	Cloud SP2
pradeep	9036161745	pradeep@gmail.com	amazon	azure
chandan	1234567890	chandu@gmail.com	amazon	azure
PRADEEP	9036161745	pradeep153426@gmail.com	amazon	azure
Revanna	9036161745	revanna2@yahoo.com	amazon	azure
vinod	0123456789	vinod@gmail.com	amazon	azure
kiran	9999568464	kiran@gmail.com	amazon	azure
thali	9036151748	thali@gmail.com	amazon	azure
suri	7894561231	suri@gmail.com	amazon	azure

#### E. User Registration Page

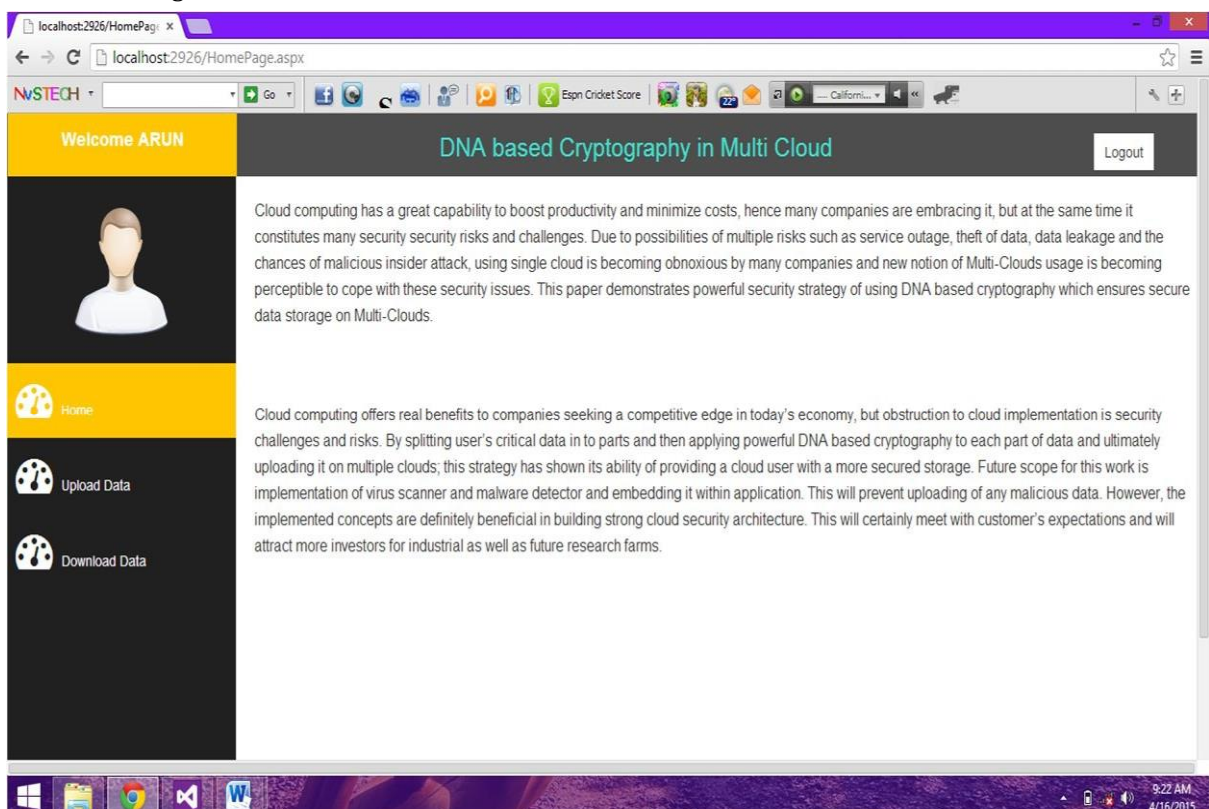


The screenshot shows a web application interface for user registration. The page has a dark background with a yellow and orange gradient. The registration form is centered and includes fields for Username, Phone Number, Cloud Service Provider (dropdown), Email, and Password. A 'Sign Up' button is at the bottom of the form. A 'Sign In' link is located at the top right of the form area.

#### F. User Sign in Page

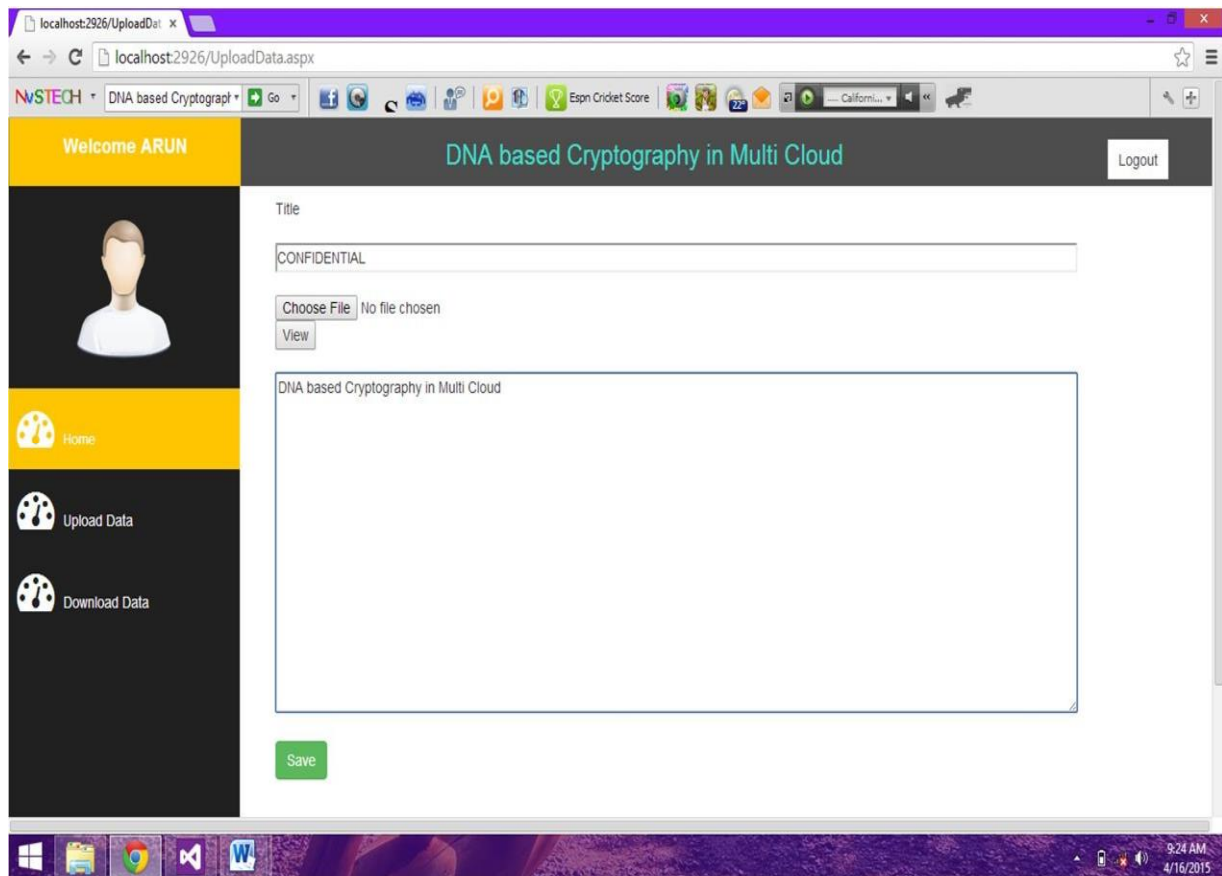


#### G. User Home Page





#### H. User Can Upload the Confidential Data



#### HARDWARE REQUIREMENTS:

- ☐ System : Pentium i3Processor.
- ☐ Hard Disk : 500GB.
- ☐ Monitor : 15"LED.
- ☐ Input Devices : Keyboard, Mouse.
- ☐ Ram : 4GB.

#### SOFTWARE REQUIREMENTS:

Operating system	:	Windows XP/7.
Coding Language	:	ASP.net, C#.net
Tool	:	Visual Studio 2017
Database	:	SQL SERVER 2016

### VIII. CONCLUSION

Cloud computing has revolutionized the way we store and process data, but it also presents numerous security challenges. While multi-clouds and DNA-based encryption are among the techniques that have been proposed to address these challenges, there is still a need for further research and development to improve the efficiency and effectiveness of these methods in practice. This paper proposed a novel DNA-based data encryption method that utilizes the natural properties of DNA to provide a practical solution to the privacy and security issues in the cloud. The proposed method employs a combination of a decimal encode rule, ASCII values, DNA molecules bases, and a complimentary rule to create a secret key that can protect the data against a range of security threats. The proposed dual access control systems are resistant to DDoS/EDoS attacks and are



"transplantable" to other CP-ABE constructions. The transparent enclave model is introduced to construct a dual access control system for cloud data sharing.

## IX. REFERENCE

- [1] M. Alzain, B. Soh and E. Pardede, "MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing", IEEE conference on Dependable, Autonomic and Secure Computing, December– 2011, pp. 784 – 791
- [2] D. Sureshraj, and V. Bhaskaran, "Automatic DNA Sequence Generation for Secured Cost-effective Multi-Cloud Storage", IEEE Conference on Mobile Application Modeling and Cloud Computing, December – 2012, pp. 1 – 6.
- [3] W. Liu, "Research on Cloud Computing Security Problems and Strategy", IEEE conference on Consumer Electronics, Communications and Networks, April-2012, pp. 1216 – 1219.
- [4] Y. Singh, F. Kandah, and W. Zhang, "A Secured Cost-effective Multi-Cloud Storage in Cloud Computing", IEEE Workshop on Computer Communications and Cloud Computing, April – 2011, pp. 619 – 624.
- [5] Joseph A Akinyele, Christina Garman, Ian Miers, Matthew WPagano, Michael Rushanan, Matthew Green, and Aviel D Rubin. Charm:a framework for rapidly prototyping cryptosystems. Journal of Cryptographic Engineering, 3(2):111–128, 2013.
- [6] Ittai Anati, Shay Gueron, Simon Johnson, and Vincent Scarlata. Innovative technology for cpu based attestation and sealing. In Workshop on hardware and architectural support for security and privacy (HASP), volume 13, page 7. ACM New York, NY, USA, 2013.
- [7] Alexandros Bakas and Antonis Michalas. Modern family: A revocable hybrid encryption scheme based on attribute-based encryption, symmetric searchable encryption and SGX. In SecureComm2019, pages 472–486, 2019.
- [8] Amos Beimel. Secure schemes for secret sharing and key distribution. PhD thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.
- [9] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In S&P 2007, pages 321–334. IEEE, 2007.
- [10] Victor Costan and Srinivas Devadas. Intel sgx explained. IACR Cryptology ePrint Archive, 2016(086):1–118, 2016.
- [11] Ben Fisch, Dhinakaran Vinayagamurthy, Dan Boneh, and Sergey Gorbunov. IRON: functional encryption using intel SGX. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, pages 765–782, 2017.
- [12] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Advances in Cryptology-CRYPTO 1999, pages 537–554. Springer, 1999.
- [13] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In ACM CCS 2006, pages 89–98. ACM, 2006.
- [14] Jinguang Han, Willy Susilo, Yi Mu, Jianying Zhou, and ManHo Allen Au. Improving privacy and security in decentralized ciphertext-policy attribute-based encryption. IEEE transactions on information forensics and security, 10(3):665–678, 2015.