iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VII **Month of publication:** July 2022

DOI: https://doi.org/10.22214/ijraset.2022.45925

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VII July 2022- Available at www.ijraset.com

DNA Based Cryptography with Dual Encryption Using Multiple Cloud

P. Prasanna[1], Ruchitha K J[2]
[1]*Associate Professor, Department of Computer Science and Engineering, PES College of Engineering, Mandya, Karnataka, India*
[2]*Department of Computer Science and Engineering, PES College of Engineering, Mandya, Karnataka, India*

Abstract: ***One recent technique in the field of cryptography is DNA cryptography. DNA can be utilised to do computations as well as encrypt data for storage and transmission. Making a DNA sequence plays a key function in DNA cryptography. Based on the data carrier and biological technology, the DNA sequence is produced. The goal of this work is to make the DNA sequence more complicated. Giving the data a high level of security is the major goal of this research. Two degrees of security are what this paper's recommended work is. The shift key is used to convert plain text to ASCII text, which is then transformed into a binary integer in the first level. Utilizing the insertion approach, change binary numbers into DNA sequences, which are then represented as cypher text. The receiver will decrypt the cypher text using the Insertion method, and the plaintext will then be displayed. The data compression of the suggested work is measured using the Shannon entropy, and the execution time is measured using the time complexity.***

Keyword: Multi-Cloud, Cloud Security, Cypher Text, DNA Cryptography.

I. INTRODUCTION

In the modern era, data size is steadily growing from gigs to trillions or even petabytes, primarily due to the development of a significant number of real data. The majority of big data is kept in cloud computing environments and is sent over the internet. Due to the fact that cloud computing offers web services, there are numerous attackers and bad users. They consistently attempt to gain access to users' private large data without the proper authorization. They occasionally substitute any bogus data for the actual data. As a result, large data security has recently generated a lot of attention. Deoxyribonucleic Acid (DNA) computing, which is based on the biological idea of DNA, is a cutting-edge emerging topic for increasing data security. In this research, an unique DNA-based data encryption method for the computing environment is described. In this case, a 1024-bit secret key is created using DNA computing, user attributes, and their Media Access Control (MAC) address. Additionally, a decimal encoding rule, an American Standard Code for Information Interchange (ASCII) value, Deoxyribonucleic acid bases, and a complementary rule are used to create the secret key, allowing the system to defend itself against a variety of security threats. Theoretical analyses and experimental findings demonstrate how effective and efficient the suggested scheme is compared to other well-known existing methods.

II. RELATED WORK

[1] compares their own multi cloud database model with Amazon cloud. They concluded that data storage and retrieval can be done more efficiently using proposed model. Their analysis also addresses data intrusion, integrity and service availability issues.

Anil Kurmus et al[2] .'s comparison of two independently developed multi-tenancy architectures, one at the kernal operating system and the other at the hypervisor level, illustrates this point. Security problems such data integrity, malevolent customers, unauthorised data access, and confidentiality are all examined as potential solutions by these two architectures.

A new word termed the rain cloud system has been defined by Sangdo Lee al.[3]. Libraries are utilised in this model to manage various CSPs. Additionally, a library interface is used to demonstrate actual data storage.

By utilising numerous CSPs with a data replication approach, current service risk or data loss, as per S.Jaya Prakash et al. [4], can be decreased. However, there should be no connection whatsoever between any CSPs. This will eliminate the security risk of a single point of contact.

III. EXISTING SYSTEM

Although cloud computing provides many advantages, there are also several security threats and challenges. Utilizing a "single cloud" provider has become less popular due to the likelihood of these dangers, including service interruption, data theft, data leaking, and the potential for malicious insider assault. The usage of many clouds, often known as "multi-clouds," "inter-clouds," or "clouds of clouds," is a materialised solution to this problem.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VII July 2022- Available at www.ijraset.com

IV. PROPOSED SYSTEM

Critical user data will be broken up into smaller pieces, with certain intriguing characteristics of biological Nucleotide sequence and data hiding principles employed, in order to improve data availability and security. The data fragments that have been encrypted with DNA will then be distributed amongst eligible Cloud Providers (CSP). Therefore, this work suggests a potential remedy for cloud security and privacy concerns.

V. METHODOLOGIES

Think about a client in a cloud-based business. The client must upload crucial data to the cloud while retaining privacy. The two steps of this method are described below.

A. Embedding Data

Firstly, we need to collect the images of people on motorcycle with helmet and without helmet along with license plate, from different source of internet.

These are the code steps:

1) If A is User data.
2) Here Binary coding rule will be applied.
3) Output of rule execution is = DNA sequence (Binary data converted to DNA nucleotides).
4) Apply base pairing rule.
5) Get = new form of A.
6) Find index of Nucleotides in DNA reference sequence.
7) Get = Cipher text.

Assume User data A = 0011011000110101 should be uploaded to the cloud. The following steps shows how user data will be convert to Cipher-Text.

DNA reference sequence is:

a) AA1 AT2 CC3 CG4 CT5 GA6 CA7 AC8 TT9 GT10 TC11 AG12 GG13 TA14 GC15 TG16
b) A = 00 11 01 10 00 11 01 01.
c) Sub-Part1 (T = 00, A = 01, G = 10, C = 11).
d) A=TCAGTCAA
e) Sub-Part2 ((A-G), (C-A), (G-T), (T-C)).
f) A=CA GT CA GG
g) Sub-Part3 (Picking Indexes); A = 710713

So finally, embedding phase is completed; User data will be sent to cloud as 710713.

B. Data Extraction

These are the code steps:

1) A = Cipher text.
2) Find the DNA reference sequence's index of nucleotides.
3) A = Previous Form of A
4) Apply the reverse base pairing rules.
5) Get = DNA Sequence.
6) Convert A to binary using binary coding rule
7) Get A= User data

Assume confidential data ssssA = 710713 should be cloud-based downloads. The process for converting cipher-text to user data is shown below.

DNA reference sequence is:

a) AA1 AT2 CC3 CG4 CT5 GA6 CA7 AC8 TT9 GT10 TC11 AG12 GG13 TA14 GC15 TG16
b) A = 710713
c) Sub-Part1 (Picking Indexes from reference sequence); A = CA GT CA GG

d) Sub- Part2 ((A-G), (C-A), (G-T), (T-C)).
e) A=TCAGTCAA.
f) Sub-Part3 (T = 00, A = 01, G = 10, C = 11).
g) A = 00 11 01 10 00 11 01 01.
So Finally, User data is extracted correctly.

C. Algorith006D

One of the newest technologies for encrypting data is DNA cryptography. Innovative inventions like DNA Computation, PCR (Polymerase Chain Reaction), Array, etc. have been employed with DNA (Animesh Hazra). Top level computation and massive data storage are features of DNA computation (Fu). A single DNA gramme has 1021 DNA bases, or 108 terabytes of data, in it. 2017 (Nirantar) (Verma, 2014). The DNA molecule's four bases—Adenine (A), Thymine (T), Cytosine (C), and Guanine (G), as well as the phosphate backbone—are depicted in Figure 1. (Lee). Assuming that the information has been encrypted using the A, G, C, and T shapes and the 0s and 1s indicated in table 1.

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

Fig-1:DNA Combination

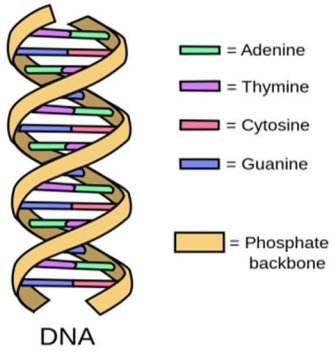


Fig-2:DNA Structure

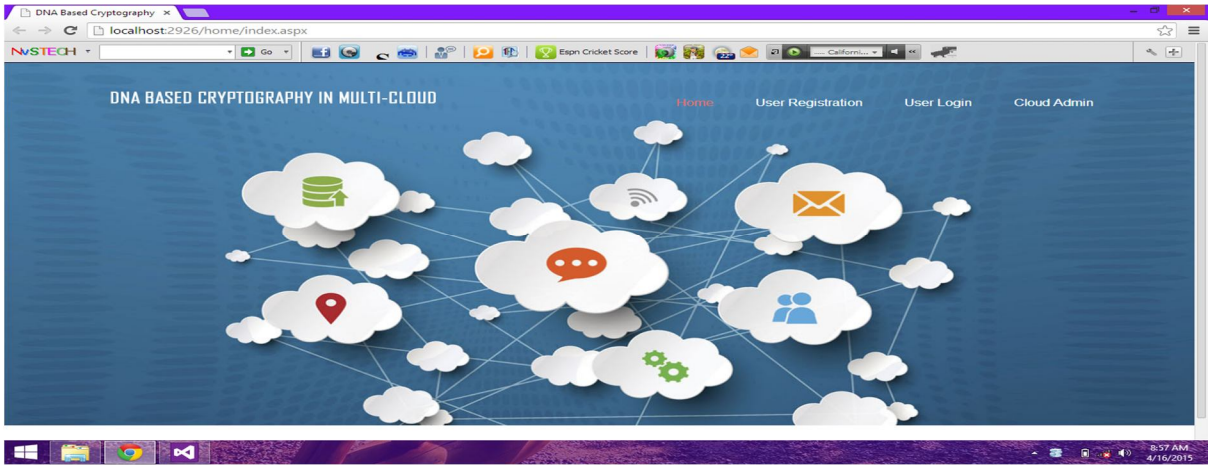
VI. WORKING OF THE SYSTEM

1) *Step 1:* Cloud service provider Adds the multiple clouds.
2) *Step 2:* User will register to the cloud by choosing primary and secondary cloud to store their data.
3) *Step 3:* At the time of registration password will get split, Encrypted and stored to the cloud.
4) *Step 4:* User will login to their workspace and upload their data, here data will get split, Encrypted and stored to the user's choice primary and secondary cloud.
5) *Step 5:* If user tries to download the data from the cloud sliced data will get joined and decrypted using DNA sequence and original data will get displayed to user.

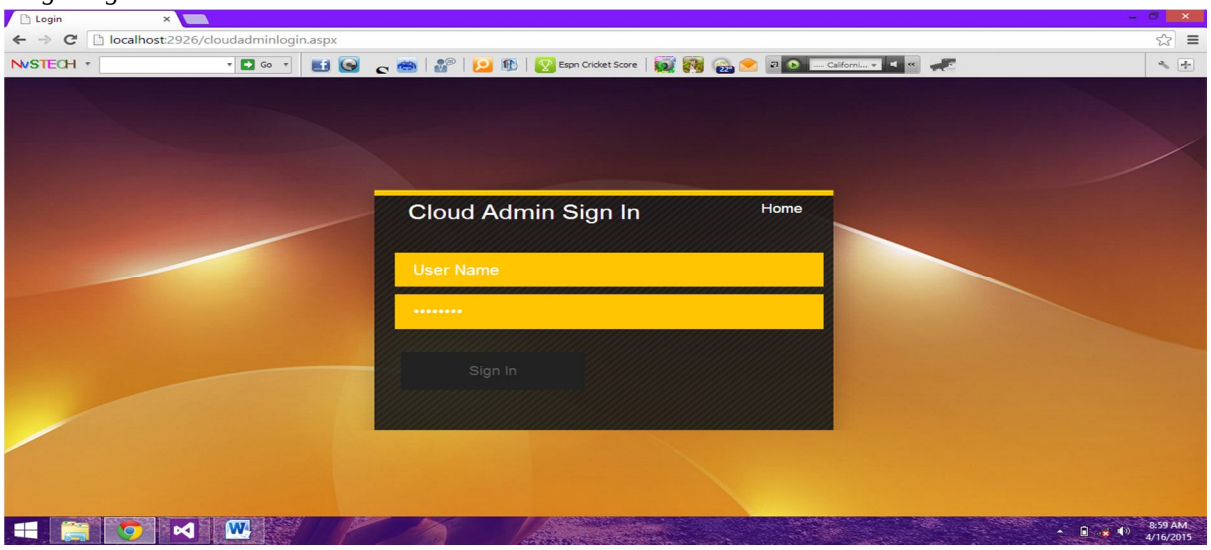
VII. RESULT AND DISCUSSION

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 .

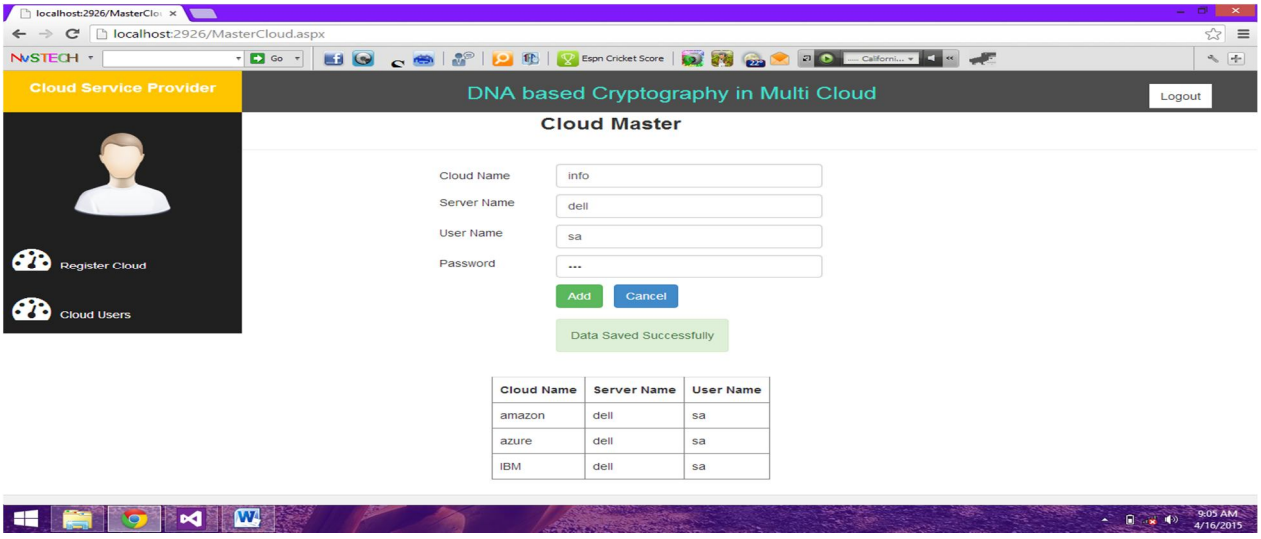
A. Home Page



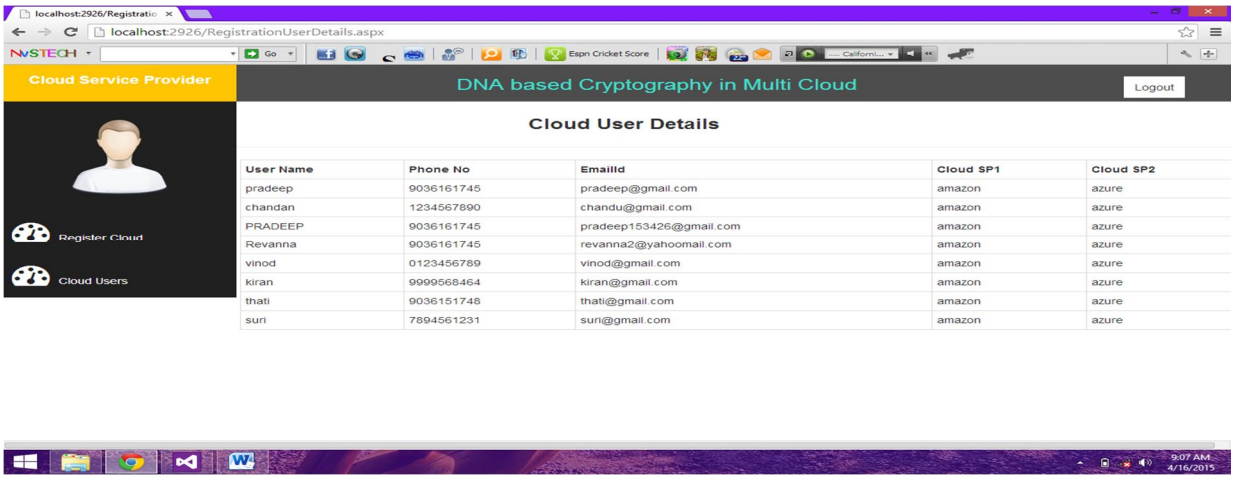
B. Admin Sign Page



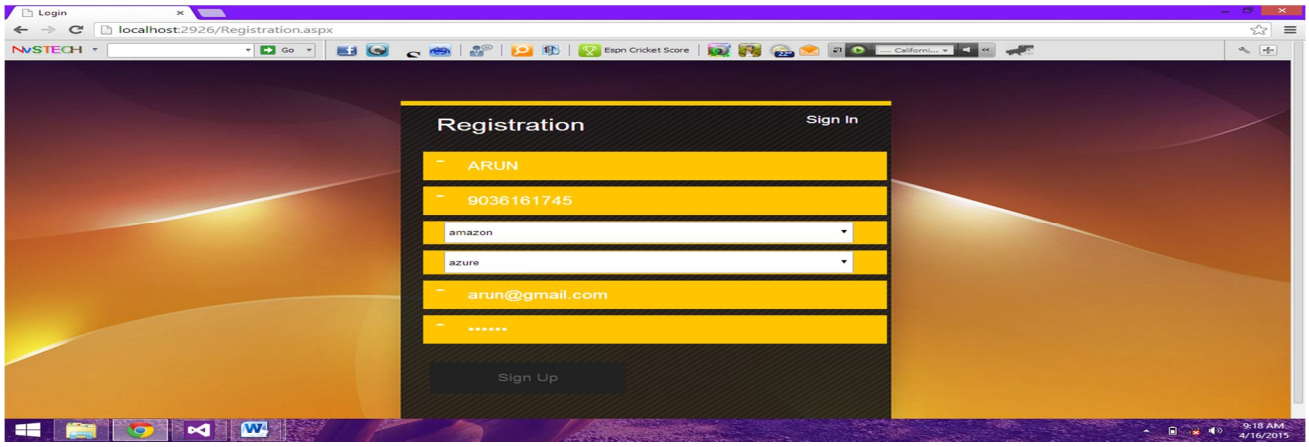
C. Admin Home Page And Create Cloud



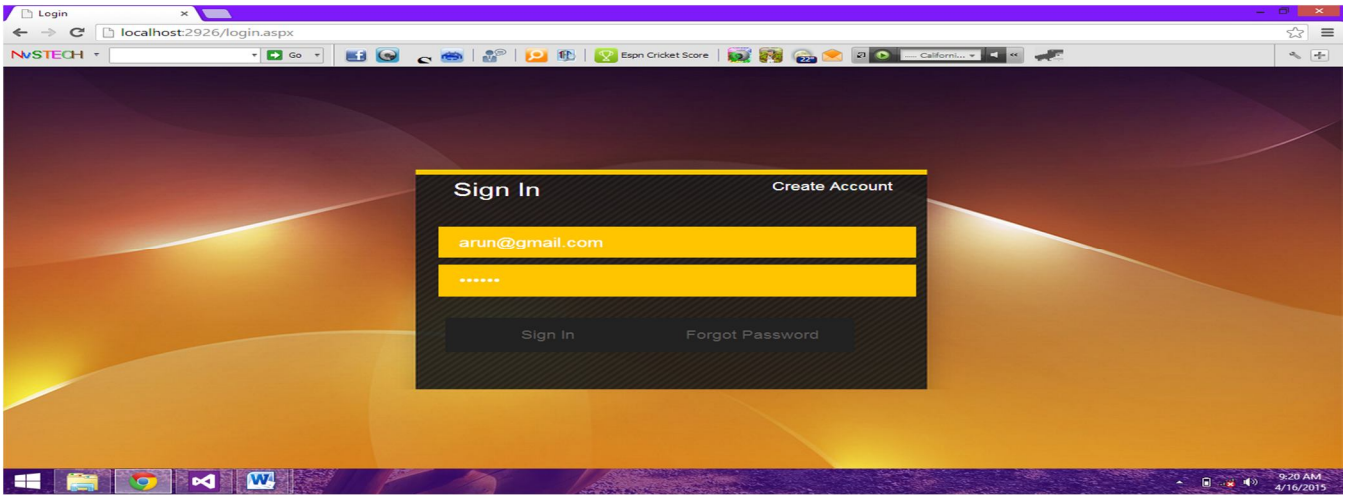
D. Admin View The Cloud User



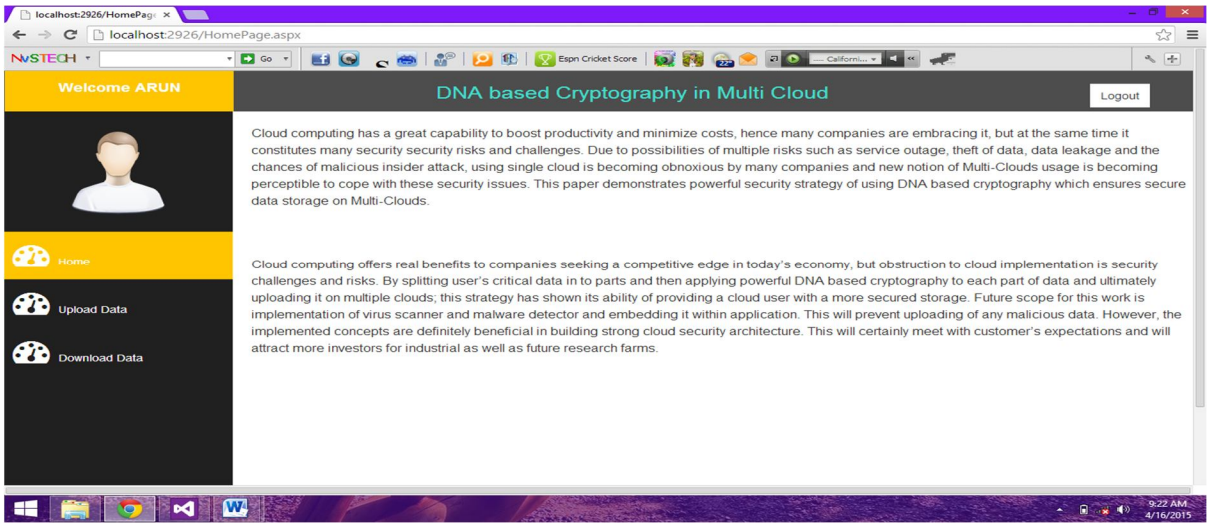
E. User Registration Page



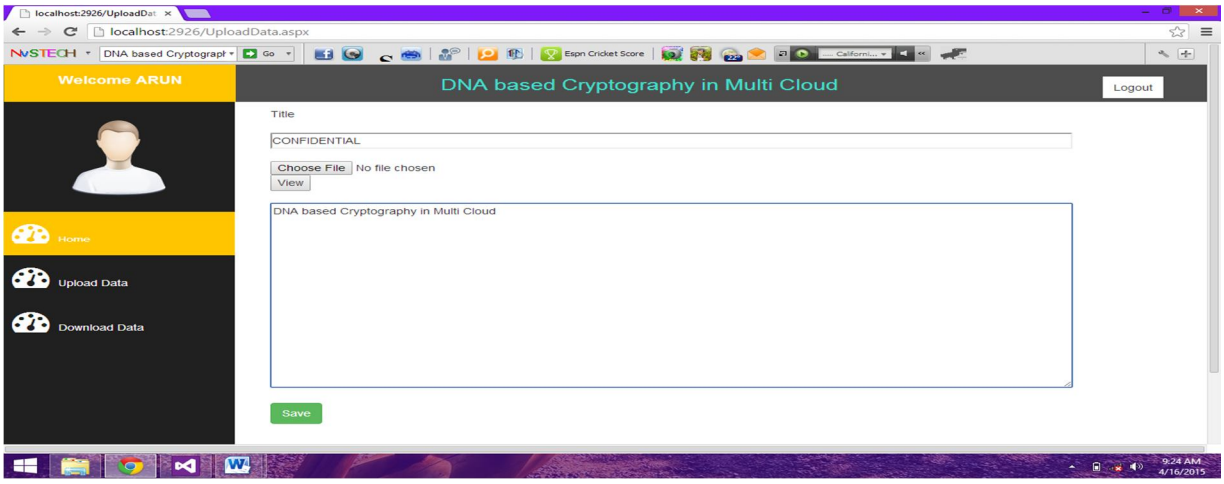
F. User Sign In Page



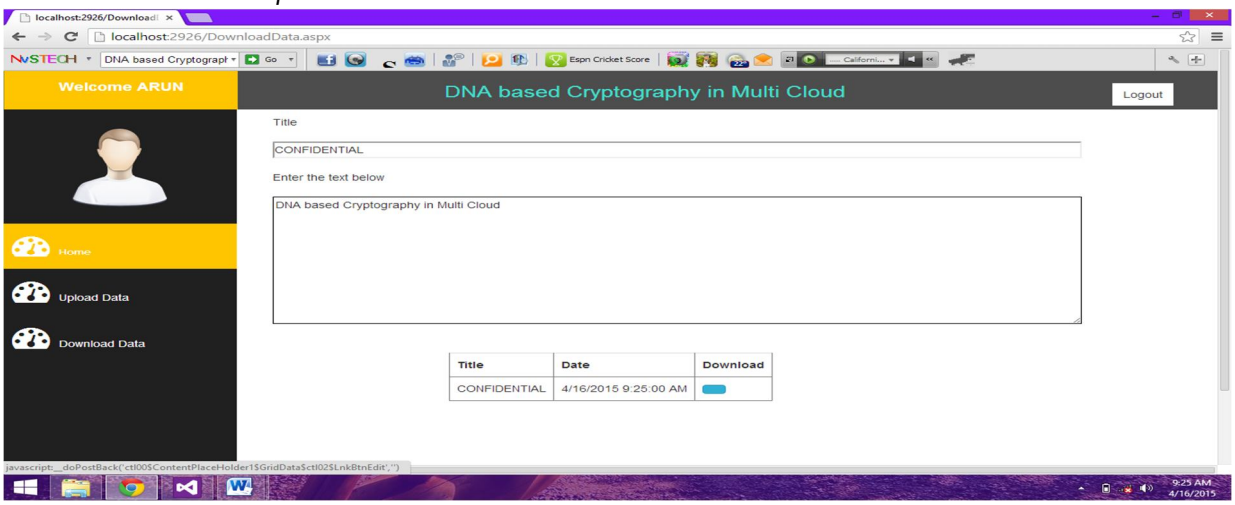
G. User Home Page



H. User Can Upload The Confidentail Data



I. User Can Download The Confidentail Data

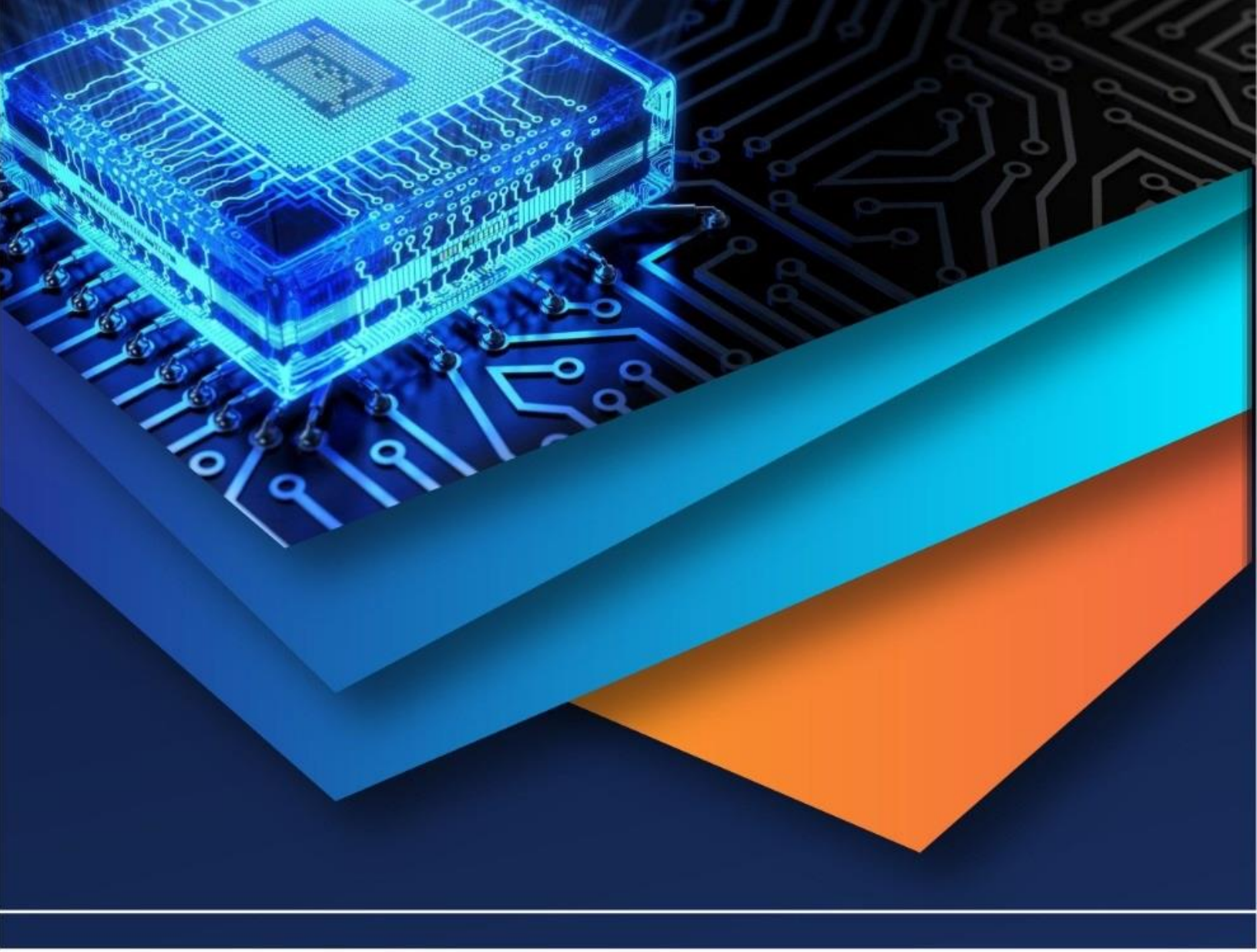


VIII. CONCLUSION

Companies looking for a competitiveness in the modern economy can gain significantly from cloud computing, but security risks and constraints make cloud implementation difficult. This technique has demonstrated its capacity to give a cloud user a more secure storage by dividing a user's vital data into pieces, applying potent DNA-based cryptography to each component of the data, and eventually uploading it to numerous clouds. However, the concepts put into practise are unquestionably helpful in creating a solid architecture for cloud security. Customers' expectations will be met, and additional investors will be drawn to industrial farms and potential research farms as a result. Future plans for this work include integrating a malware detector and virus scanning into the application. This will stop any malicious uploads.

REFERENCES

[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", IEEEE 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.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY