Abstract/Summary of Bachelor's Thesis/Final Year Project

The thesis work titled "**Secure Data Storage On Multi-Cloud Using DNA Based Cryptography**" was aimed to demonstrate a powerful security strategy of using DNA based cryptography, which ensures secure data storage on multi-cloud. The system designed was three-tier architecture: User, Application Provider (Server) and Cloud Service Provider. The system proposes to process the encryption algorithm at the user/client side by using its own resources to enhance data security and reduce the load on the server. Let D be the binary format of data which client has to upload over the cloud space. The first phase of encryption is responsible for using DNA base pairing rule to produce D', which is a nucleotide sequence. Base pairing rule is applied to convert binary bit pairs to representing nucleotides using reference DNA sequence. The second phase applies the DNA complementary rule to increase the complexity of hidden data to produce D'' from D'. The role of the third phase is to extract the index of the nucleotide couple from the DNA reference string. All the DNA nucleotide couples in D'' are replaced by their respective indexes to form secret data D'''. While extracting the original data, the reverse algorithm is applied. The encrypted file is then divided into different parts, which are stored over different cloud spaces to give immense security to the client's critical data. To increase data availability, different divided parts are combined and stored such that even if at all any cloud has failed still the data can be retrieved from the remaining clouds.

For project report, research paper and more information click on the following link:
https://drive.google.com/drive/folders/1eJ3dEvCnkRI2f4Wvv-eRgrfuqOo1FjlT?usp=sharing