

**SStoreEasyY**  
**A PROJECT REPORT**  
***Submitted by***  
**Sahil Darji[1721BECE30024]**  
**Smit Gautami[1721BECE30033]**  
***In fulfilment for the award of the degree***  
***of***  
**BACHELOR OF ENGINEERING**  
**In**  
**COMPUTER ENGINEERING**



**LDRP INSTITUTE OF TECHNOLOGY AND RESEARCH,**  
**GANDHINAGAR**  
**Kadi Sarva Vishwavidyalaya, Gandhinagar**  
**2020 - 2021**

# LDRP Institute of Technology and Research

## Computer Engineering Department



### CERTIFICATE

This is to certify that the Project Work entitled **“SStoreEasyY”** has been carried out by **Sahil N. Darji(1721BECE30024)** under our guidance in fulfilment of the degree of Bachelor of Engineering in Computer Engineering (7<sup>th</sup> Semester) of Kadi Sarva Vishwavidyalaya University, Gandhinagar during the academic year 2020-21.

**Guide:**

**Dr. Bela Shrimali**  
**Internal Guide,**  
**LDRP ITR.**

**Dr. Shivangi Surati**  
**Head of the Department,**  
**LDRP ITR.**

## **TABLE OF CONTENTS**

Table of Contents	iii
List of Figures	v
List of Tables	viii
List of Graphs	ix
Acknowledgement	x
Abstract	xi
1. Introduction	1
1.1. What is Cloud?	1
1.1.1 Cloud Definition	1
1.1.2 Cloud Architecture	1
1.1.3 Characteristics of Cloud Computing	2
1.2. Need of Security in Cloud	2
1.3. Cryptography	3
1.3.1 Types of Cryptography	4
1.3.2 Hybrid Cryptography	5
1.3.3 Need of Hybrid Cryptography	6
1.4. Problem Statement	7
1.5. Plan of their work	7
2. Technology & Literature Survey	8
2.1. Title “Security and Privacy in Cloud Computing”	9
2.1.1 Cloud Characteristics	9
2.1.2 Security Challenges	9
2.1.3 Current Strategies	10
2.1.4 Conclusion	10
2.2. Title “Secure Data Sharing in Clouds”	11
2.2.1 SeDaSC	11
2.2.2 Conclusion	12
2.3. Title “A Study of Encryption Algorithms”	12
2.3.1 RSA	13
2.3.2 DES	13
2.3.4 AES	13
2.3.5 RC4	14
2.3.6 Blowfish	14
2.3.7 Conclusion	15
3. System Design	15
3.1 Software Requirements	16
3.2 Hardware Requirements	16
3.3 Proposed Model	17
3.4 Flow Diagram	17
3.5 Research Algorithm	18
3.5.1 AES	20
3.5.2 DES	20
3.5.3 RC4	21
3.5.4 RSA	21
	22
	22

3.6 Additional Algorithm Approach	23
3.6.1 Layered Encryption	23
3.6.2 Hybrid Cryptosystem	24
4. System Diagrams	25
4.1 Class Diagram	25
4.2 Use Case Diagram	26
4.3 Data Flow Diagram	27
4.4 Sequence Diagram	28
5. Test Plan	29
5.1 Test Files	30
5.2 Processing Time	30
5.2.1 Encryption and Decryption Time for AES	31
5.2.2 Encryption and Decryption Time for Hybrid Algorithm	31
5.2.3 Encryption and Decryption Time for Layered Algorithm	32
5.2.4 Encryption and Decryption Time for Hybrid Cryptosystem	32
5.3 Conclusion	33
6. Results and Performance Analysis	34
6.1 Comparison of Cryptographic Algorithms	35
6.2 Algorithms Testing	35
6.2.1 AES Testing	36
6.2.2 Hybrid Encryption Testing	37
6.3 Comparison of Encryption Algorithms Testing Data	37
6.4 Comparison of Hybrid Encryption with Layered Encryption	38
6.5 Application Screenshots	39
6.5.1 File Encryption	40
6.5.2 Download Key	41
6.5.3 Decryption Types	41
6.5.4 Download File	42
7. Conclusions	43
7.1 Conclusions	45
7.2 Applications	45
7.3 Future Scope	46
7.4 References	46

## LIST OF FIGURES

<b>S.NO.</b>	<b>Title</b>	<b>Page No.</b>
1	Figure 1.1 - Overall view of Cloud Computing	1
2	Figure 1.2 - Cloud Architecture	2
3	Figure 1.3 - Areas in Data Security	4
4	Figure 1.4 - Security Algorithms	5
5	Figure 1.5 - Classification of Cryptographic Algorithms	5
6	Figure 1.6 - Encryption of data using Hybrid Technique	6
7	Figure 2.1 - Challenges in Data Security on Cloud	9
8	Figure 2.2 - Basic Model of SeDaSC	10
9	Figure 2.3 - Encryption time with key compute	11
10	Figure 2.4 - AES Design	13
11	Figure 3.1 - Hybrid Encryption	15
12	Figure 3.2 - Encryption Flow Diagram	16
13	Figure 3.3 - Decryption Flow Diagram	16

14	Figure 3.4 - Basic Flow AES	17
15	Figure 3.5 - The SubBytes Step	18
16	Figure 3.6 - The ShiftRows Step	18
17	Figure 3.7 – The MixCloumns Step	18

18	Figure 3.8 - AddRoundKey Step	19
19	Figure 3.9 - DES Flow Diagram	19
20	Figure 3.10 - RC4 Schematic Representation	20
21	Figure 3.11 - RC4 Lookup Stage	21
22	Figure 3.12 - RSA working example	22
23	Figure 3.13 – Layered Encryption	23
24	Figure 3.14 - Layered Decryption	23
25	Figure 3.15 – Encryption using Hybrid Cryptosystem	24
26	Figure 3.16 - Decryption using Hybrid Cryptosystem	24
27	Figure 5.1 - Time to encrypt 10mb file using AES	30
28	Figure 5.2 - Time to decrypt 10mb of file using AES	31
29	Figure 5.3 - Time to encrypt 10mb file using Hybrid Algorithm	31
30	Figure 5.4 - Time to decrypt 10mb file using Hybrid Algorithm	32

31	Figure 5.5 - Time to encrypt 10mb file using Layered Algorithm	32
32	Figure 5.6 - Time to decrypt 10mb file using Layered Algorithm	33
33	Figure 5.7 - Time to encrypt 10mb file using Hybrid Cryptosystem	33
34	Figure 5.8 - Time to decrypt 10mb file using Hybrid Cryptosystem	34
35	Figure 6.1 – File Encryption	43
36	Figure 6.2 – Download Key	44
37	Figure 6.3 – File Decryption	44
38	Figure 6.4 – Download File	45
39	Figure 6.5 – Decryption Types	45
40	Figure 6.6 – Hybrid Decryption	46

## LIST OF TABLES

<b>S.NO.</b>	<b>Title</b>	<b>Page No.</b>
1	Table 6.1 - Comparison of different Encryption Algorithms	35
2	Table 6.2 -AES Encryption Time	36
3	Table 6.3 - AES Decryption Time	37
4	Table 6.4 - Hybrid Encryption Time	38
5	Table 6.5 - Hybrid Decryption Time	39
6	Table 6.6 - Comparison of Different Algorithms	40
7	Table 6.7 - Comparison of Different Encryption Approaches	41
8	Table 6.7 - Comparison of Different Decryption Approaches	42



## LIST OF GRAPHS

S.NO.	Title	Page No.
1	Graph 6.1 – Encryption using AES	36
2	Graph 6.2 - Decryption using AES	37
3	Graph 6.3 – Encryption using Hybrid Algorithm	38
4	Graph 6.4 - Decryption using Hybrid Algorithm	39
5	Graph 6.5 - Time Comparison between AES and Hybrid Encryption Algorithm	40
6	Table 6.6 - Time Comparison between AES and Hybrid Decryption Algorithm	41
7	Table 6.7 - Comparison between Hybrid, Hybrid Cryptosystem and Layered Encryption	42
8	Table 6.7 - Comparison between Hybrid, Hybrid Cryptosystem and Layered Decryption	43

## ACKNOWLEDGEMENT

With immense pleasure we would like to present this report on our topic “SStoreEasyY”. We are thankful to all that have helped us a lot for successful completion of our project and providing us courage for completing the work.

We are thankful to our Head of the Department **Dr. Shivangi Surati**, our project guide **Dr. Bela Shrimali** for providing encouragement, constant support and guidance which was of a great help to complete this project successfully.

We thank our Dearest parent, who encourages us to extend our reach with their help and support, we have been able to complete this work. We are also thankful to all my friends who directly or indirectly have been helpful in some or the other way.

**Sahil Darji (1721BECE30024)**

**Smit Gautami (1721BECE30033)**

## **ABSTRACT**

The cloud is a cutting-edge stage that conveys virtualization, dynamic asset pools and high accessibility. Since distributed computing lays on web, security issues like information security, protection, security, secrecy and verification are experienced. In order to get rid of these, an assortment of mechanisms and encryption algorithms are utilized in various blends. On the comparable terms, we made utilization of hybrid encryption with the utilization of cross breed cryptographic calculations to upgrade the security of information on cloud. We plan at investigating different amalgamations of encryption algorithms, in view of various execution constraints to reason a hybrid calculation which can anchor information more effectively on cloud.