**Secure Cloud Simulation**

A Report submitted

by

**Varun Dhall (1301021173)**

**Deepank Srivastava (1301021048)**

**Arshdeep Kaur Gulati (1301021036)**

**Under the Guidance of**

**Mr. Prashant Kumar**

**Assistant Professor**

**Computer Science & Engineering Department**



In partial fulfilment of the requirements for the Degree of

**BACHELOR OF TECHNOLOGY**

in

**COMPUTER SCIENCE & ENGINEERING,**

**DIT UNIVERSITY, DEHRADUN**

(State Private University through State Legislature Act No. 10 of 2013 of Uttarakhand and approved by UGC)

**Mussoorie Diversion Road, Dehradun, Uttarakhand – 248009**

**CERTIFICATE**

This is to certify that the project report entitled **“Secure Cloud Simulation”** being submitted by **Varun Dhall, Deepank Srivastava and Arshdeep Kaur Gulati** in partial fulfillment for the award of the Degree of Bachelor of Technology in Computer Science and Engineering to the DIT University (Established vide Uttrakhand Act No. 10 of 2013 and recognized by UGC under section 2(f) of the UGC Act, 1956) is a record of bona fide work carried out by them under my guidance and supervision.

The results embodied in this project report have not been submitted to any other University or Institute for the award of any Degree or Diploma.

Dr. M. L Garg

**Head of Department**

**CSE Department**

Mr. Prashant Kumar

**Assistant Professor**

**CSE Department**

**CANDIDATE/S DECLARATION**

I hereby certify that the work, which is being presented in the report/ project report, entitled **Secure Cloud Simulation,** in partial fulfilment of the requirement for the award of the Degree of **Bachelor of Technology** and submitted to the institution is an authentic record of my/our own work carried out during the period *September-2016* to *April-2017* under the supervision of Mr. Prashant Kumar, Assistant Professor - CSE Department.

Date: Signature of the Candidates

This is to certify that the above statement made by the candidates is correct to the best of my /our knowledge.

Date: Signature of the Supervisor

**TABLE OF CONTENTS**

Title Page No.

ABSTRACT ...................................................................................................................V

ACKNOWLEDGEMENT…………………………………………………………….vi

LIST OF TABLES........................................................................................................vii

LIST OF FIGURES......................................................................................................xi

ABBREVIATIONS……………………………………………………………………x

NOTATIONS…………………………………………………………………...…….xi

**CHAPTER 1 INTRODUCTION**

1.1 Purpose .............................................................................................................

1.2 Objective...........................................................................................................

1.3 Motivation……………………….……………………………………………

1.4 Definition and Overview……………………………………………………….

**CHAPTER 2 OVERALL DESCRIPTION**

2.1 Project Perspective ...................................................................................…….

2.2 Project Functions…….………..........................................................................

2.3 E-R and DFD Diagrams ……………………………………………………..

2.4 Constraints and Assumptions….......................................................................

**CHAPTER 3 SYSTEM REQUIREMENTS**

3.1 External Interface Requirement.........................................................................

3.1.1 Hardware interface…………………………………………………......

3.1.2 Software Interface…………. ................................................................

3.2 Functional Requirement ...................................................................................

3.3 Non-functional Requirement..............................................................................

3.4 Hardware and Performance Requirement…………………………………….

**CHAPTER 4 CONCLUSION AND FUTURE WORK**

4.1 Conclusions ....................................................................................................

4.2 Scope for Future Work ...................................................................................

**REFERENCES** ……………………………………………………..………………

**ABSTRACT**

Currently, data security and privacy policy has been regarded as one of the biggest concerns in cloud computing. Data stored at remote storage is unsafe and susceptible to get hacked. Due to this, users do not trust their data over the cloud. Cloud consumers wants an assurance that they can access their data where ever they want and no one else is able to get it. Moreover, authentication of users over the cloud is also an important concern to think about. After doing the survey and studying the research papers it is found that the major security concerns of cloud computing includes Data leakage, Distributed Denial of Service (DDOS). The data security can be improved by implementing various symmetric key algorithms so that data on the server is stored in a manner that even if a person gets access then also he can't open the original data. As it needs to be decrypted. Apart from storage security, authorised access of users enable may help in avoiding DDOS as only genuine users will have access to the cloud.

A hybrid model is proposed which is a mixture of elliptical curve cryptography and symmetric key algorithm. ECC is used to achieve the process of user's verification and to keep the private data secure. AES algorithm is used which allow the user to store and access their data securely to the cloud by encrypting the data in the client side and decrypting the data after downloading from the cloud. Since the private key is owned by the user of the data, no one can decrypt the data, even though the hacker can get the data through some approaches. Moreover, user will securely authenticate itself by using different input parameters at the time of login to the cloud server. This scheme can make users assure about the security of data stored in the cloud. Here, we will apply an ECC and ECDH algorithm that provide same level of security as of other public key crypto systems with less key size and strengthens the security of the algorithm. The whole prototype of the proposed solution would benefit by enabling a proper access mechanism to avoid unauthorised access to the information system and a secure storage to allow access of data over the cloud network.

**ACKNOWLEDGEMENT**

We wish to express our deep sense of gratitude and indebtedness to Assistant Professor Prashant Kumar, Department of Computer Science and Engineering, DIT University, for introducing the present significant topic and for his inspiring guidance, constructive criticism and valuable suggestion throughout this project work.

We also extend our sincere thanks to all our friends who have patiently helped us in accomplishing this undertaking. We also thank Mr. Sarvesh Shukla, Assistant Professor, Department of Computer Science and Engineering, DIT University for his constant support throughout the project work.

We would also like to thank people like Qin Liu, Guojun Wang, Uma Somani, Kanika Lakhani, Manish Mundra for conducting high level research and publishing such significant research papers related to this topic.

**LIST OF TABLES**

**Table No. Title Page No.**

2.3.4.1 Class Table for Student Info database………………………………….19

2.3.4.2 Class Table for Result database..………………………..........................20

**LIST OF FIGURES**

**Figure No. Title Page No**.

2.1 Main Screen ………………………………………………………….......6

2.2 Registration Screen ………………………………………………………. 7

2.3 Login Screen……………………………………………………………….8

2.4 Sem 1 &2 Tabbed Result Screen…………………………………………..9

2.5 Sem 3 &4 Tabbed Result Screen…………………………………………10

2.6 Sem 5 &6 Tabbed Result Screen…………………………………………11

2.7 Sem 7 &8 Tabbed Result Screen…………………………………………12

2.8 CGPA Calculator…………………………………………………………13

2.9 Downloads Section……………………………………………………….14

2.10 Level 0 DFD……………………………………………………………...15

2.11 Level 1 DFD……………………………………………………………...16

2.12 Level 2 DFD……………………………………………………………...17

2.13 Use- Case Diagram………………………………………………………..18

**ABBREVIATIONS**

SDK Software Development Kit

API Application Programming Interface

ECC Elliptic Curve Cryptography

DFD Data Flow Diagram

ER Entity Relationship

IMAP Internet Message Access Protocol

RAM Random Access Memory

KB Mega Byte

MB Mega Byte

GB Giga Byte

**NOTATIONS**

A < B A is less than B

A > B A is greater than B

A ≤ B A is less than or equal to B

A ≥ B B is greater than or Equal to B EK Encryption Key

DK Decryption Key

Fn *n*th Fibonacci number

In the identity matrix of order n

N Set of Positive Integers W Set of Whole Numbers Z Set of Integers

Z+ Set of Positive Integers

Zn Set of non-negative integers less than n