**Secure Cloud Simulation**

A Synopsis 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**

**TABLE OF CONTENTS**

Title Page No

1. INTRODUCTION 1
2. FEASIBILITY STUDY 3
3. METHODOLOGY 4
4. FACILITIES REQUIRED 5
5. INNOVATIVENESS AND USEFULNESS 6
6. CURRENT STATUS OF DEVELOPMENT 6
7. REFERENCES 7

**Introduction**

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.

**Problem Statement:**

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.

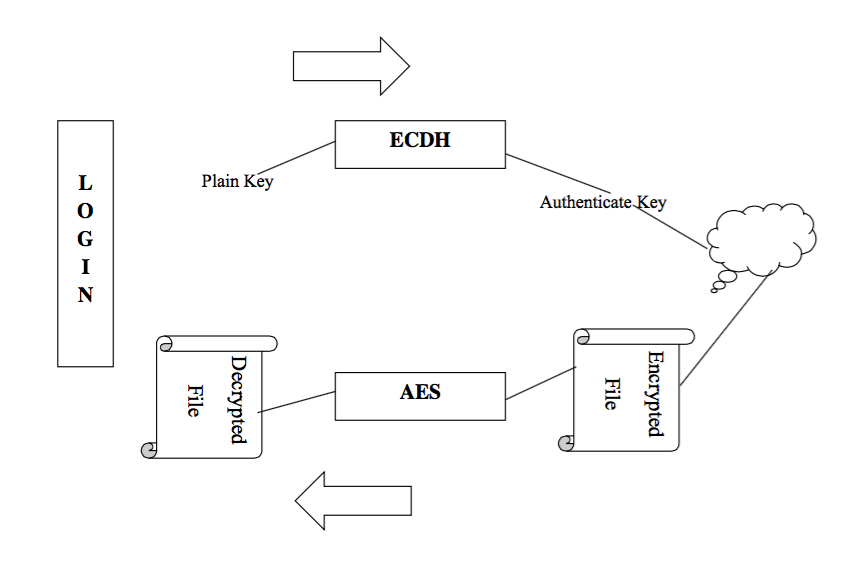
**Overview of Proposed Solution:**

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.

Benefits are:

* Proper access mechanism to avoid unauthorised access to the information system.
* Secure storage and access of data over the cloud.

1



**Overall Display of Project Implementation**

2

**Feasibility Study**

The Project simulates a model that is already quite common for consumer apps like email and photo sharing, and for certain business applications. But in this project, we present a way to secure the data using different compression and encryption algorithms and to hide its location from the users that stores and retrieves it. As with the Internet, on-demand applications have grown so ubiquitous that almost every business user interacts with at least one, whether it's an email service, a Web conferencing application, or a file hosting system. The data is stored at multiple places over the information space (over the Internet). It sounds similar to file hosting websites which stores the data that is being uploaded by different users and can be retrieved using proper authentication. The only difference is that the system for which project is targeted is an application based system like which will run on the clients own system. This application will allow users to upload file of different formats with security features including Encryption and Compression over the cloud securely.

The uploaded files can be accessed from anywhere using the application which is provided. We believe this system serves as a foundation for future work in integrating and securing information sources across the World Wide Web.

3

**Methodology**

As computer science students, our task is to figure out which platform components are going to allow us to build all of these features. The system architecture shows the core design of the application. The system serves the purpose of file hosting and hence requires a server that holds data. Multiple clients can log in to the server and share files. The system should work in the flow as shown below:

* User should register on website and download the application and install it.
* User has to log in through the application and performs operation user wants.
* User should register on website and download the application and install it.
* Database is in 3rd normal form.
* Data compression by using zipping up-to 70%.
* Data size is 4MB with full binary support.
* Existing system is updated from 3 tiers to N tier that improve the security.
* 256 bit AES encryption algorithm is used for file security.
* Proposed system is multi-cloud compatible that is it is independent of backend services and infrastructure.

All the quality attributes are taken into consideration and it comprises of all persistent systems standards.

4

**Facilities Required**

**Hardware Requirements:**

* Processor – i3/i5/i7 x64 Bit Minimum 2.
* Hard Disk – 8 GB + at least 2 GB for Relational Database System
* Memory – 2 GB RAM minimum, 4 GB RAM recommended
* Internet Access

**Software Requirements:**

* Linux OS, Ubuntu 14.04 Preferred
* JDK 7 or above
* NetBeans IDE
* Relational Database Server, MYSQL Preferred
* Apache Tomcat Server

5

**Innovativeness & Usefulness**

IaaS (Infrastructure as a service) is the foundation layer of the Cloud Computing delivery model that consists of multiple components and technologies. Each component in Cloud infrastructure has its vulnerability which might impact the whole Cloud’s computing security. Cloud Computing business grows rapidly despite security concerns, so collaborations between Cloud parties would assist in overcoming security challenges and promote secure Cloud Computing services. In this project, we will investigate the security challenges that associate it with IaaS implementation and deployment. The security issues presented here concern the security of each IaaS component in addition to recent proposed solutions. Our future research vision will focus on two directions to provide confidentiality, integrity, and secure Infrastructure management for IaaS service. Finally, a prototype will be implemented to demonstrate the system feasibility and performance.

**Current State of Development**

Currently, we are in the design phase of our project. We have successfully completed our survey and research about various security challenges faced in cloud computing industry. After this, we analysed and compared various algorithms and techniques that could be used to solve data leakage and other security issues. We are focusing on the implementation of this prototype using Java technologies to enable portability and platform independence. We believe that we’ll be able to complete the implementation, deployment and load testing of the solution in the given time.

6

**References**

1. Qin Liu, Guojun Wang, and Jie Wu“Efficient Sharing of Secure Cloud Storage Services” 2010 .10th IEEE International Conference on Computer and Information Technology (CIT - 2010).
2. Uma Somani, Kanika Lakhani, Manish Mundra“Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing” 2010 IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).
3. Ashutosh Kumar Dubey 1, Animesh Kumar Dubey 2, Mayank Namdev3, Shiv Shakti Shrivastava4 “Cloud-User Security Based on R SA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment “in 2011.
4. Xiang Tana, Bo Aib“The Issues of Cloud Computing Security in High-speed Railway “in 2011.
5. Arthur Rahumed, Henry C. H. Chen, Yang Tang, Patrick P. C. Lee, and John C. S. Lui “A Secure Cloud Backup System with Assured Deletion and Version Control” 2011 International Conference on Parallel Processing Workshops.
6. Eman M.Mohamed and Sherif EI-Etriby “Randomness Testing of Modem Encryption Techniques in Cloud Environment” in year 2008.

7