SECURE FILE STORAGE USING HYBRID CRYPTOGRAPHY

Project report submitted
in partial fulfillment of the requirements for the Degree of
Bachelor of Engineering
in
Computer Science& Engineering

By

SUBHADEEP DAN (BE/6069/16)

VIKASH KUMAR (BE/6093/16)

ANKIT KUMAR MISHRA (BE/6096/16)

Project Supervisor

Dr. Kamta Nath Mishra

Dept. of CSE, BIT Mesra, Off Campus Deoghar

BIRLA INSTITUTE OF TECHNOLOGY, MESRA

OFF CAMPUS DEOGHAR

Deoghar – 814142, Jharkhand

CERTIFICATE

This is to certify that **Mr. Subhadeep Dan, Mr. Vikash Kumar** and **Mr. Ankit Kumar Mishra** have developed the project titled "**Secure File Storage Using Hybrid Cryptography**" in my supervision and guidance. To the best of my knowledge the project work is original.

(Signature with Date)

Dr. Kamta Nath Mishra

Guide& HOD

Department of Comp. Sc. &Eng.

Birla Institute of Technology, Ranchi

Off Campus – Deoghar, Jharkhand

DECLARATION

We hereby declare that the project entitled **Secure File Storage Using Hybrid Cryptography** which is being submitted in partial fulfillment of the requirement for award of the Degree of Bachelor of Engineering in Computer Science and Engineering to BIRLA INSTITUTE OF TECHNOLOGY, MESRA, OFF-CAMPUS, DEOGHAR is an authentic record of our own work done under the guidance of Dr. Kamta Nath Mishra.

The matter reported in this Project has not been submitted earlier for the award of any other degree.

Date: 10-06-2020

Place: BIT Deoghar

ACKNOWLEDGEMENT

We sincerely express indebtedness to esteemed and revered guide **Dr. Kamta Nath Mishra,** Head of Department of Computer Science and Engineering for his invaluable guidance, supervision, and encouragement throughout the work. Without his kind patronage and guidance, the synopsis would not have taken shape. Also, we thank him for providing the computer lab facility. We would like to express our sincere regards to him for advice and counseling from time to time.

We owe sincere thanks to all the faculties in Department of Computer Science and Engineering for their advice and counseling time to time.

Date: 10-06-2020

Place: BIT Deoghar

Subhadeep Dan

Vikash Kumar

Ankit Kumar Mishra

TABLE OF CONTENTS

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, authorized 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 unauthorized access to the information system and a secure storage to allow access of data over the cloud network.

1. INTRODUCTION

1.1 PURPOSE

Cloud Computing is the style of computing where the resources are provided as services on internet. There are three types of services in Cloud Computing which are used for the deployment of the application on the cloud. Data on the cloud will become more scalable, Reliable and Secure. The big players in Cloud Computing are Amazon, Google, Microsoft and IBM. Cloud Computing is based on five attributes such as Shared Resources, Scalability, Pay as U use, Elasticity and Self Provisioning of Resource. Most of the enterprises shifting their applications on to the cloud owing to its speed of implementation and deployment, improved customer experience, scalability, and cost control. The services in Cloud Computing are **SaaS**, **PaaS, laaS** amongst which we are using PaaS and laaS service for deployment of Application on the Cloud in our Project. This service exhibits five essential characteristics such As Rapid Elasticity, Resource Pooling, on demand Self-service, Broad Network Areas. Data is being transmitted between two clouds so in order to secure the data most of the systems use the combination of techniques, including:

• Encryption- It is used to encode the data in such a way that third party will not be able to hack that data.

• Authentication- It is used to create a separate user ID and Password so that only the authorized users will able to access the data.

•Separation of duties- In which accessibility is provided to all the users according to their priority.

These security parameters are achieved due to which the performance will gets increased and therefore the Security is obtained up to higher extent. Data security and privacy risks have become the primary concern for people to shift to cloud computing. Cloud Computing is mainly used for the improving the data handling capability where the services and the resources will be delivered continuously when and where required due to which the Cloud computing is in great demand. However there still exist many problems in cloud computing today, a recent survey

shows that data security and privacy risks have become the primary concern for people to shift to cloud computing Cloud is the free space where the application is being saved securely and the services are being provided continuously when and where required.

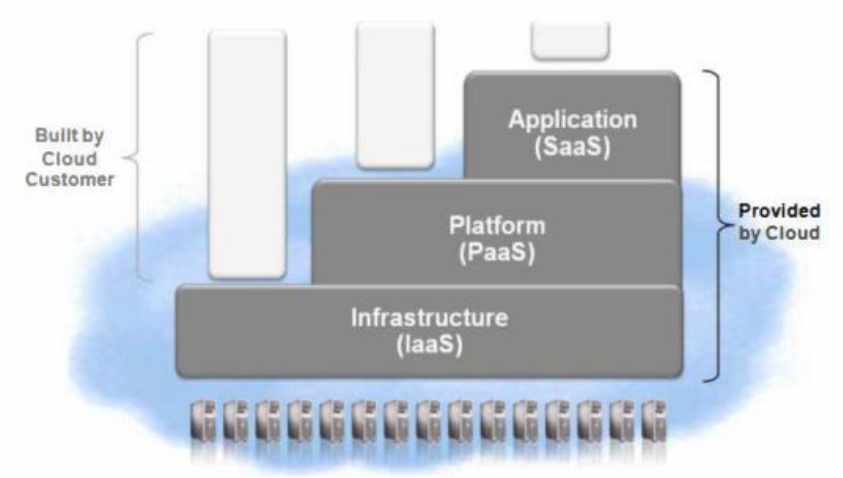
Cloud Deployment Models:

A. *Public Cloud*: The Cloud infrastructure is made available for the large industry group and general public provided by single service provider.

B. *Private Cloud*: The Organization can store the data on private Cloud. The main Advantage of this Cloud is Security of Data and Quality of Service.

C. *Community Cloud*: The Cloud Infrastructure is shared by many Organizations.

D. *Hybrid Cloud*: Two or more Clouds combine to form Hybrid Cloud.



Cloud Characteristics:

A. *Easy Use*- Most Cloud Provider will offer the Internet interfaces which are much simple so user can easily access the cloud services.

B. *Ubiquitous Network Access*- Cloud provides services through the standard terminal such as phones, Laptops, Mobiles.

C. *On demand Services*- Cloud is a pool of resources and services so we can get the services and resources by paying particular amount as required.

D. *Business Model*-Cloud is a Business Model because it is pay per use of service or resource.

E. *Pay as U Used* - Users have to pay for only the Resources they are using. Whenever the users need some resources then they have to pay for the particular resource as and when required.

1.2 OBJECTIVE

The primary goal of this project is to provide and simulate an effective solution to face the challenges and solve security issues that exists in cloud computing. Cloud Computing is the impending need of computing which is used for the IT Industries It is one of the hottest topic in research areas. Scalability and Flexibility increases for the computing services. Cloud Computing is the fastest growing technology for IT Industry. The Information is being transmitted via the network therefore security is one of the main problems or issue. The Application is deployed on the Cloud and for the secure transmission of the data we will be using ECC Algorithm in our project because of its advantages in terms of CPU utilization, time for Encryption and Key Size. This Project will explore the deployment of Application on the Cloud and increases the security level by implementing ECC & ECDH Algorithm, and AES Algorithm for secure file handling and Encryption.

1.3 MOTIVATION

Need of data security is an essential issue in the domain of computing traditionally. There are various algorithms are developed in order to improve the security of data, but they having their

own issues. Now in these days the traditional algorithms are not much suitable for providing security over the untrusted communications and data exchange.

ECC is more and more considered as an attractive public-key cryptosystem for mobile/wireless environments. One of the other recent public key cryptosystems is Elliptic Curves Cryptography use for security. In recent times, the majority of e-commerce applications are designed using asymmetric cryptography to assure the authentication of the concerned parties. Compared to traditional public-key cryptosystems like RSA or Diffie-Hellman, ECC propose equivalent security with smaller key sizes; these results in faster calculation, lower power expenditure, as well as memory and bandwidth savings. ECC is peculiarly useful for mobile devices, which are typically particular in terms of their CPU, power and network connectivity.

Therefore, a new encryption standard is required that can fulfil the current need of security meanwhile that is extendable according to the need. The proposed work includes the development of new hybrid algorithm using ECC, ECDH and AES algorithms along with encryption techniques.

1.4 DEFINITION AND OVERVIEW

Cloud Computing is the primitive change happening in the field of Information Technology. It uses the internet technologies for delivery of IT - enabled capabilities 'as a service' to any needed users. Cloud computing enables users to access resources using internet, from anywhere at any time without worrying about technical/physical management and maintenance concern of the original resources. In its description for cloud characteristics The US National Institute of Standards and Technology (NIST) defines as cloud characteristics the following: On-demand self-service, Ubiquitous network access, Resource pooling, Rapid elasticity (resources can be scaled up and down easily), Metered service (resources' usage is measured) and Pay-As-You-Consume business models. Google Apps is an important example of Cloud computing; it enables to access services through the browser and brought into effective action on millions of machines over the Internet. One of the most prominent service offered by cloud computing is cloud

storage. Cloud storage is simply a term that refers to on line space that you can use to store your data. In more strict way, cloud storage is a service model in which data is maintained, managed and backed up remotely and made available to users over a network.

Software as a service (SaaS)

The cloud provider deploys, configures, maintains and updates the operation of the software applications on a cloud infrastructure so that the services are provisioned at the expected service levels to cloud consumers. The cloud consumers have limited administrative control of the applications.

Platform as a service (PaaS)

The Cloud Provider manages the computing infrastructure for the platform and runs the cloud software that provides the components of the platform, such as runtime software execution stack, databases, and other middleware components. The PaaS Cloud Provider typically also supports the development, deployment and management process of the PaaS Cloud Consumer by providing tools such as integrated development environments (IDEs), development version of cloud software, software development kits (SDKs), deployment and management tools.

Infrastructure as a service (IaaS)

The Cloud Provider acquires the physical computing resources underlying the service, including the servers, networks, storage and hosting infrastructure. The Cloud Provider runs the cloud software necessary to makes computing resources available to the IaaS Cloud Consumer through a set of service interfaces and computing resource abstractions, such as virtual machines and virtual network interfaces.

The whole idea and definition of this project lies in its name i.e. **Secure Cloud**, which aims at providing and simulating an effective solution to face the challenges and solve security issues that exists in cloud computing. But first we should look at some of the frequently occurring issues in cloud computing mostly during the transmission of data. Some of them are discussed below:

A. *Encryption*- The message send by the sender i.e. the original message is being encrypted in such a way that third party will not be able to hack or misuse the data.

B. *Intrusion Detection and Prevention*- Data that is being entered and going out of the Network has to know.

C. *Separation of Duties*- Due to the insufficient communication between the expertise System misconfiguration takes place.

D. *Location of Data*- Every Organization will have different requirements and their access control on their data to be placed. A level of security is required to fulfil the customer need.

Sharing of Cloud Infrastructure could lead to the privacy issues. The Location of data could influence the privacy obligations. For storage and processing of data. Data leakage could also occur due to failure of security access rights. In order to secure the data stored on the cloud various security Algorithms are present which will help to encrypt the data before transmission in order to protect the valuable data from the hackers.

One of the better solution for maintain the security is cryptography which is basically used for protecting the data. **Public Key Cryptography**- In this cryptography different keys are used for Encryption and Decryption. **Secret Key Cryptography**- A key which is used for Encryption as well as Decryption is called Secret Key Cryptography. There are many Security Algorithms Each Algorithm have their own properties such as Key Size, Throughput, Performance, Encryption Decryption Time etc. By Comparing the Encryption Algorithms, we found out that ECC Algorithm is one of the best Algorithm which is having the high level of Security and better performance.

2. RELATED WORK

This chapter surveys previous work done in the field of major security concerns in cloud computing and how to ensure data privacy using various cryptographic algorithms.

2.1 Major Security Concerns of Cloud Computing

- **Data Leakage**

  Innately, when moving to a cloud there is two changes for customer's data. First, the data will store away from the customer's local machine. Second, the data is moving from a single-tenant to a multi-tenant environment. These changes can raise an important concern that called data leakage. Because of them, Data leakage has become one of the greatest organizational risks from security standpoint.

- **Cloud Security Issues**

  Innately, Internet is communication infrastructure for cloud providers that use well-known TCP/IP protocol which users' IP addresses to identify them in the Internet. Similar to physical computer in the Internet that have IP address, a virtual machine in the Internet has an IP address as well. A malicious user, whether internal or external, like a legal user can find this IP addresses as well. In this case, malicious user can find out which physical servers the victim is using then by implanting a malicious virtual machine at that location to launch an attack. Because all of users who use same virtual machine as infrastructure, if a hacker steals a virtual machine or take control over it, he will be able to access to all users' data within it. Therefore, The hacker can copy them into his local machine before cloud provider detect that virtual machine is in out of control then the hacker with analysis the data may be find valuable data afterward.

    - **Attacks in Cloud**

      Nowadays, there are several attacks in the IT world. Basically, as the cloud can give service to legal users it can also service to users that have malicious

purposes. A hacker can use a cloud to host a malicious application for achieve his object which may be a DDoS attacks against cloud itself or arranging another user in the cloud. For example, assume an attacker knew that his victim is using typical cloud provider, now attacker by using same cloud provider can sketch an attack against his victim. This situation is similar to this scenario that both attacker and victim are in same network but with this difference that they use virtual machines instead of physical network.

➔ DDoS Attacks against Clouds

Distributed Denial of Service (DDoS) attacks typically focus high quantity of IP packets at specific network entry elements; usually any form of hardware that operates on a Blacklist pattern is quickly overrun and will become in out of - service situation. In cloud computing where infrastructure is shared by large number of clients, DDoS attacks make have the potential of having much greater impact than against single tenanted architectures. If cloud has not plenty resource to provide services to its costumers then this is may be cause undesirable DDoS attacks. Solution for this event is a traditional solution that is increase number of such critical resources. But serious problem is when a malicious user deliberately done a DDoS attacks using bot-net.

➔ Cloud against DDoS Attacks

DDoS attacks are one of the powerful threats available in world, especially when launched from a botnet with huge numbers of zombie machines. When a DDoS attack is launched, it sends a heavy flood of packets to a Web server from multiple sources. In this situation, the cloud may be part of the solution. it's interesting to consider that websites experiencing DDoS attacks which have limitation in server resources, can take advantage of using cloud that provides 24/7 more resource to tolerate such attacks. In the other hand, cloud technology offers the benefit of flexibility, with the ability to provide resources almost instantaneously as necessary to avoid site shutdown.

2.2 Data Privacy in Cloud

Sharing of Cloud Infrastructure could lead to the privacy issues. The Location of data could influence the privacy obligations. For storage and processing of data. Data leakage could also occur due to failure of security access rights[5]. In order to secure the data stored on the cloud various security Algorithms are present which will help to encrypt the data before transmission in order to protect the valuable data from the hackers. One of the better solution for maintain the security is cryptography which is basically used for protecting the data.

A) **Public Key Cryptography**- In this cryptography different keys are used for Encryption and Decryption.

B) **Secret Key Cryptography**- A key which is used for Encryption as well as Decryption is called Secret Key Cryptography.

There are many Security Algorithms Each Algorithm have their own properties such as Key Size, Throughput, Performance, Encryption Decryption Time etc. By Comparing the Encryption Algorithms we found out that ECC Algorithm is one of the best Algorithm which is having the high level of Security and better performance.

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, authorized access of users enable may help in avoiding DDOS as only genuine users will have access to the cloud.

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. PROJECT SPECIFICATION

3.1 EXTERNAL INTERFACE REQUIREMENT

3.1.1 User Interface

- Platform – Desktop or Mobile browser
- Display – 1024x768 or higher, 1366x768 recommended
- Colour – 16 million coloured display
- JavaScript enabled browser.
- Latest Video and supported graphics drivers.

3.1.2 Hardware Interface

- Processor – i3/i5/i7 x64 Bit Minimum 2 Ghz.
- Hard Disk – 8 GB + at least 2 GB for Relational Database System
- Memory – 2 GB RAM minimum, 4 GB RAM recommended
- High Speed Internet Access
- LAN Connection with Ethernet.

3.1.3 Software Interface

- Linux / Windows OS, Ubuntu 16.04 Preferred
- JDK 7 or above
- NetBeans IDE
- Relational Database Server, MYSQL Preferred
- Apache Tomcat Server

3.2 FUNCTIONAL REQUIREMENTS

The functional requirement part discusses the functional behavior that should be possessed by the system. Each requirement maps to a higher-level function that transforms the given set of input data into output data. The functional requirements can be identified as the modules involved. These modules perform separate functions based on the given input and return output data for the next level. Each module acts as an independent entity acting on its own but the output collected is just an intermediate data for other modules.

Different types of functional requirements possessed by the system are:

1. Introduction Module
2. Registration Module
3. Key Exchange Module
4. ID Generation Module
5. Login Module

Module 1: Introduction Module

- Purpose – A brief introduction. It is invented to be engaging and communicate the theme of the cloud application to the user.
- Inputs – No input is necessary.
- Outputs – Immediately load the Main Menu Screen (Registration Screen).

Module 2: Registration Module

- Purpose – The central point after connection establishment. The menu responds to user clicks and details are sent to the server.
- Inputs – Username, Mobile Number, Email, DOB fields are displayed, submit button.
- Outputs – Control is passed to key exchange page with a random registration created.

Module 3: Key Exchange Module

- Purpose – For ECCDH equivalent key exchange.
- Inputs – Secret Private Key for exchange.
- Outputs –ECDH Key is generated and OTP sent to mail ID.

Module 4: ID Generation Module

- Purpose – For user ID generation. Generation of user ID. Accessing the cloud storage. Fresh OTP sent to email ID.
- Inputs – OTP from email ID in the text field. User ID and OTP Request.
- Outputs – Random user ID is generated. OTP verification and redirecting to user account.

Module 5: Login Module

- Purpose – To check credentials of the user and log him in if they are correct and grant the access to their account.
- Inputs – User ID and the OTP sent to the user's email ID.
- Outputs – Immediately load the Profile Screen if the credentials match.

3.3 NON - FUNCTIONAL REQUIREMENTS

A careful specification and adherence of non-functional requirements such as performance, security, privacy and availability are crucial to the success or failure of any software system.

3.3.1 Performance Requirements

- The capability of the application depends on the performance of the servers. Anyone can use the application easily because of good GUI.
- The application can take any number of users provided the database size is large enough. It depends on the available memory space in database.
- On mobile devices and laptops, the battery is a scarce and valuable resource. The battery should remain maximally available for the application to perform well. Your application may therefore fall by the wayside or even get uninstalled by the user, if it drains too much battery.
- The text font size may need to be adjusted up (for high resolution screens) or down (for low resolution screens) so as to keep the text readable.

3.3.2 Safety Requirements

- The layout may need to be taken care of and adjusted to increase or decrease the spacing between and around labels and widgets shown on the screen so as to prevent them from getting clustered together on high-res screens or spaced apart too much on low-res screens.

- Any images used in the project have to be provided in two different versions: a large size/high resolution version and a small size/low resolution version so that it properly fills the amount of physical space available on the screen.

3.3.3 Security Requirements

- Although security is the utmost priority and has been taken care the most but care must be taken against virus and malware threats.
- This application will be available for all the users within the Internet. The system server should be up for 365 days and the downtime should be minimized in case of any attack or difficulties.
- Firewall should be used on the user's system to prevent any suspicious activity.

3.3.4 Software Quality Attributes

- 24x7 availability of the system with suitable updating at regular interval of time. To maintain integrity of the data and in order to ensure the security of the database by asking them to sign up for the application.
- Form validation so that only real users access the system. An error message should be displayed in case of improper working of the application.
- Email -ID entered should be valid as OTP is sent to that Email ID.
- The application can be accessed at any place that has Internet connectivity.
- Always save the data before closing the website.
- An error message should be displayed in case of improper working of the application.
- 24 hours availability of internet connection is required.

4. PROBLEM DESIGN

4.1 ALGORITHM/METHODOLOGY

We have in mind a hybrid model proposed which is a mixture of Elliptical Curve Cryptography and a 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 allows the user to store and access their data securely in 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 hackers can get the data through some approaches, they will not be able to access it. 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 provides same level of security as of other public key cryptosystems 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

The model would be hosted on a website. The website is designed keeping in mind an average user so that he can understand the functioning easily and does not have to hassle with the complex design of the website. The simple design of the website makes it very easy for any user to access it easily and make full use of the product.

- **Elliptic Curve Cryptography(ECC)**:

  Elliptic curve systems were first proposed in 1985 by Neal Koblitz and Victor Miller. An Elliptic curve over a field K have a set of points(Xi,Yi) in a plane. The set is finite and is denoted by E. It is one of the most secure Algorithm. ECC is a public key cryptography Algorithm in which each and every user has its own pair of private and public key. Group Operator is an important one in ECC and is denoted by the symbol '+'. The Standard form of ECC is given by y2 =x3 + ax + b for some fixed values for parameters a and b. The security of ECC Algorithm depends on the ability of computation of new points on the curve and then the encryption of these points as information is to be exchanged between the end users. Group Operator is used to find P which is one of the point on the curve. Again, this operator proceeds the computation as P+P, P+P+P, ... , which makes it very difficult for the hacker to hack the data.

- **Key Agreement using ECDH Algorithm**:

  Both clouds i.e. Cloud A and Cloud B will agree for the data which is being transmitted The Agreement between the two parties will takes place only when both the keys are same.

  I) A will select an integer XA = k1 as his/her private key. The public key for A will be Y A = XA x P, which implies that when the private key is an ordinary integer, the public key is a point like P.

  2) B does exactly the same thing it selects an integer XB = K2 as his/her private key, with the public key for B being YB =XB x P. Then both the parties exchange their public keys.

  3) A computes the session key by KA = XA x YB = kl x k2 x P

  4) B computes the session key by KB = XB x YA = k2 x kl x P. Obviously, KA = K

  This proves the Agreement for exchanging the Data between two parties and the generation of public and private key.

- **Key Generation:**

  Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

  Now, we have to select a number**'d'** within the range of **'n'**.

  Using the following equation we can generate the public key

  - **Q = d * P**

  d = The random number that we have selected within the range of (**1 to n-1**). **P** is the point on the curve.

  'Q' is the public key and**'d' is the private key.**

  Algorithm generates both the public key and private key. Here Sender will be used to encrypt the data and receiver i.e. B is used to decrypt the data by using its own private key.

- **Encryption:**

  Let 'm' be the message that has been sent from the sender A to B. Sender A will encode the message and on the way of transmission only the encryption will take place and for the transmission of data only few nano-seconds will be required to travel the data to receiver.

- **File Encryption using AES**

  AES is the Advanced Encryption Standard, a United States government standard algorithm for changing the plain text to cipher text i.e. encrypting and decryption the data. The proposed system uses AES to encrypt the files with a secret key to secure the uploaded files. The user has to enter the private key and select the file for encryption. Once the file is encrypted, during the process of decryption, the user has to enter the AES key which was generated during encryption.

ALGORITHM

```
Algorithm Start (FileName, Private Key){
        Browse Files
        Enter private key
}
Algorithm Encrypt() {
        Convert to State Array
        AddRoundKey()
        SubBytes()
        ShiftRows()
        MixColumns()
        Key Expansion
}
Algorithm Decrypt {
        Convert to State Array
        AddRoundKey()
        InvSubBytes()
        InvShiftRows()
        InvMixColumns()
        Key Expansion
}
```

4.2 PROJECT FUNCTIONS

- The **landing page** of the web application – the very first page which is visible when the app is launched in the browser of the user's system. This page lets the user know about the application and let the user to choose between first time registration and login features. Along with this, the page contains tabs for download and upload section also. It contains, app logo, tag line and makes the user aware about the goal of the application is short period of time and enhances aesthetic value.

- The **Registration Page** of the application which is displayed when user is using the application for the first time or does not possess a user account.

  The form here takes user's full name, email address, mobile number, DOB and gender as input to store user's information and validate the user before giving access to the app data. It first checks for all possible errors in the credentials on the client side itself using regular expressions and pattern matching. Later, if the data passes all the test cases, it is sent to server side to validate and store the details in the database to create a working profile of the user.

- The **Key Exchange** part of the application, uses ECC algorithm therefore, public key and private key both are generated. Here Sender will be used to encrypt the data and receiver i.e. B is used to decrypt the data by using its own private key. The form here takes, registration number along with secret key for successful key exchange.

- Then there is the 3rd stage of Registration process itself. Here ECDH key agreement has been automatically generated successfully and **OTP (one time password)** is sent to the email address given by the user on stage one of the registration. The app takes OTP as input and after proper validation of both the fields, it passes the control to the next stage of new user registration.

- On successful validation, the application generates a unique **User ID**. The user is requested to save this ID as, once the registration is done, the user will be using just the User ID generated here and the secret key entered earlier to use all the features and perform validation further in the application. The new user registration completes here and now the user can easily login to access his profile and use all the features of the application.

- After that, the **Login page** of the application which is loaded when the user clicks on the login tab button. The page consists of a simple form which inputs the User ID of the user generated during registration process and the OTP which is immediately sent to the user's

email address as soon as he clicks on ‘Request for OTP’ button in the form. Later, both the values in the fields are validated over the server with the values in the database and if successful the user is taken to the next page that is Dashboard of the application, else error is generated.

- The **Dashboard Page** of the application. When the user is able to successfully login into the app for the first time, he is taken to the My Account section where he is shown the current details of his account stored in the database and is given an opportunity to update any field if required and click on submit button to save. The dashboard page serves as a navigating page as from here the user can go-to encryption, decryption download and upload sections and can log out from the app if the work is done.

- The **File Encryption** part of the application. If the user wishes to upload a file in the cloud application and encrypt it to ensure security, he would hit the encryption tab. Next he is asked to enter the Encryption key which is actually the same secret key entered at the time of registration also. After that, he is asked to select the file to be uploaded from his local system on which the application is running. Lastly, click on submit to process the encryption and saving of file.

- . Now after the encryption and uploading of the file is completed, the user can go to the decryption section, enter the respective AES key that was generated and given to him, and select the file to download. After this, the chosen file is decrypted and ready for download. The downloading would start as soon as the user hits the download button.

4.3 CLASS TABLES AND UML DIAGRAMS

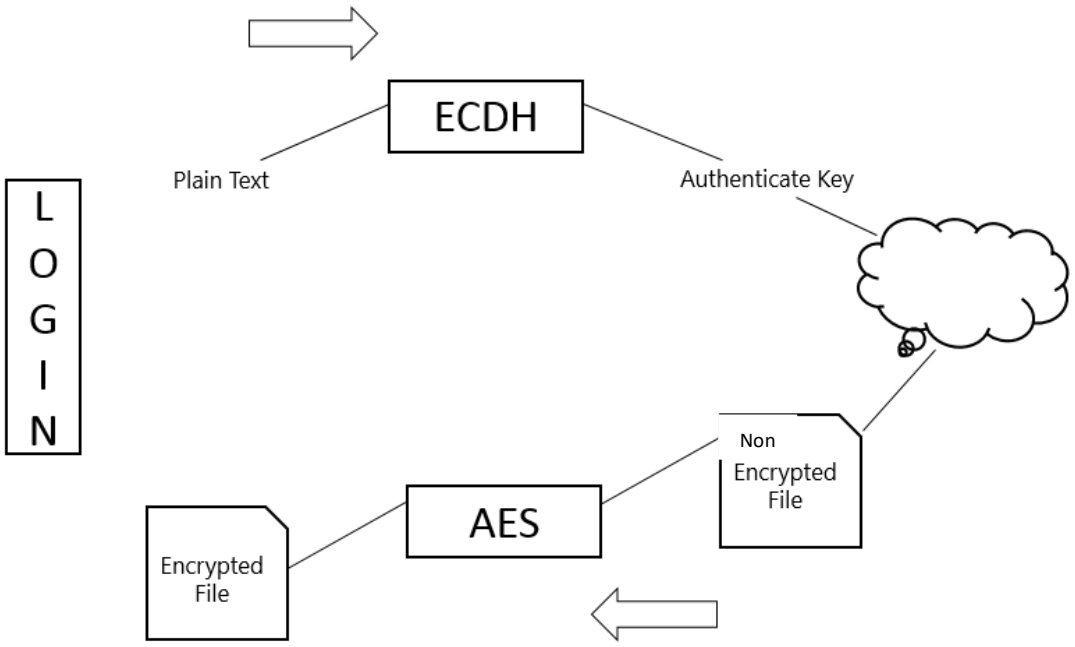


Fig. 1

Overall display of the project

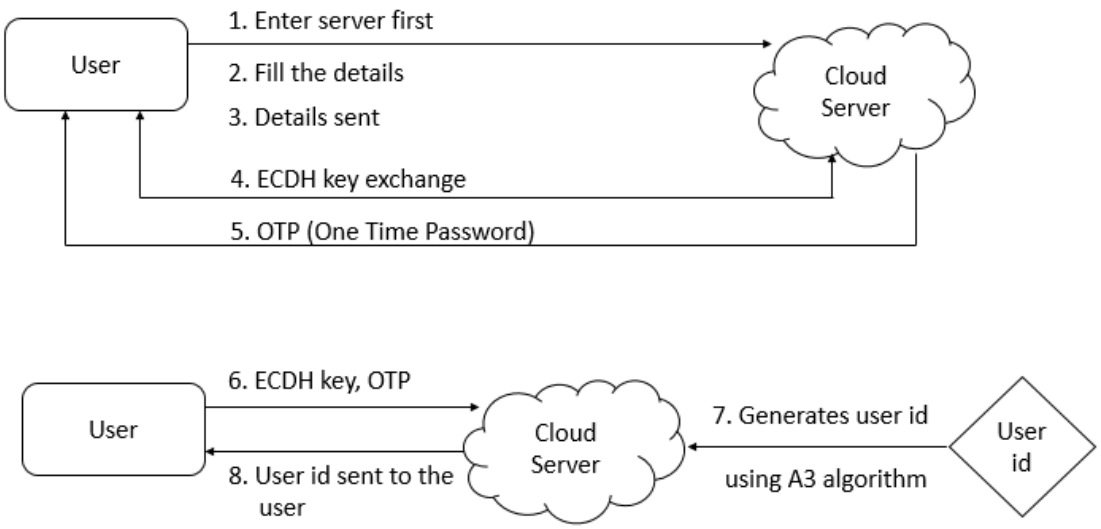


Fig. 2

Overall architecture with component description and dependency details

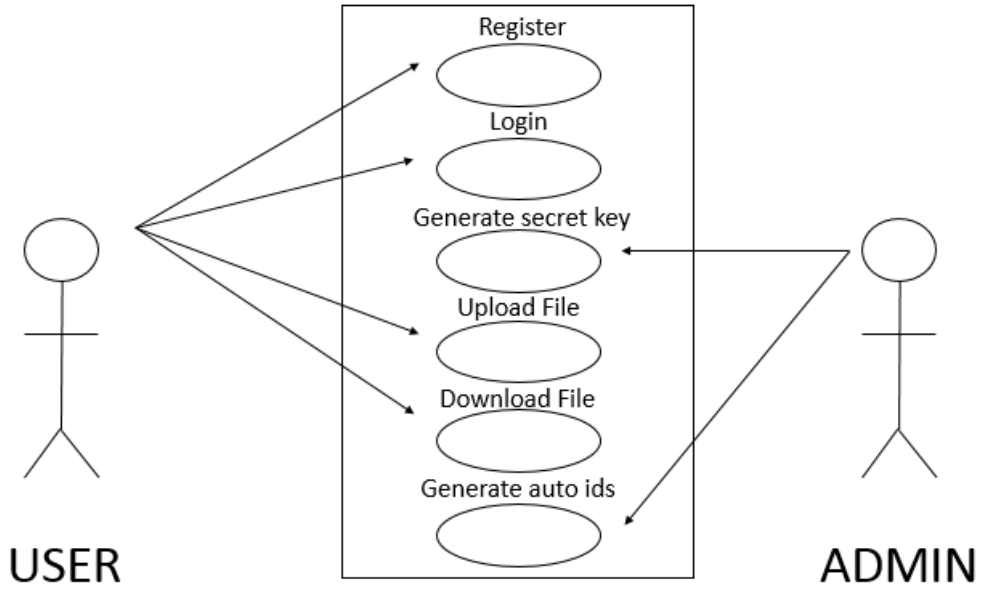


Fig. 6

User-Case Diagram

4.3.2. CLASS TABLES

AUTO_ID		
NAME	**DATA TYPE**	**NULL/ NOT NULL**
FORM_NAME	**Varchar(50)**	**Null**
PREFIX	Varchar(100)	Null

Fig. 7

FILES		
NAME	**DATA TYPE**	**NULL/ NOT NULL**
ID	Bigint(20)	Not Null
USER_ID	Varchar(50)	Null
FILE_NAME	Varchar(100)	Null
FILE_PATH	Varchar(255)	Null
CREATED	Datetime	Null
F_STATUS	Char(1)	1
ENCRYPTED_AES_KEY	Varchar(255)	Null
PUBLIC_KEY	Varchar(255)	Null
PRIVATE_KEY	Varchar(255)	Null

Fig. 8

USERS		
NAME	**DATA TYPE**	**NULL/ NOT NULL**
USER_ID	Varchar(20)	Not Null
GEN_USER_ID	Varchar(200)	Null
NAME	Varchar(100)	Not Null
EMAIL	Varchar(100)	Null
MOBILE	Varchar(20)	Null
DOB	Varchar(100)	Null
GENDER	Varchar(50)	Null
USER_KEY	Varchar(50)	Null
SECRETU	Varchar(200)	Null
USER_OTP	Varchar(10)	Null
UTYPE	Varchar(20)	'user'
U_STATUS	Char(1)	1
CREATED	datetime	Null

Fig. 9

USER_LOGIN		
NAME	**DATA TYPE**	**NULL/ NOT NULL**
USER_ID	Varchar(20)	Not Null
OTP	Varchar(10)	Not Null
CREATED	DATE	NOT NULL

Fig. 10

4.4 CONSTRAINTS AND ASSUMPTIONS

Following are the constraints of Secure File Storage Using Hybrid Cryptography:

- The software is only available on the web.
- The project implements a security model and shows the simulation.
- To use this model in real time a lot of modifications will be needed.
- The project will be tested against a certain set of test cases only.

Following are the assumptions:

- The user has good knowledge of operating a computer and web application.
- The computer system has internet and/or LAN connection enabled.
- It is mandatory for the internet to be turned on and active.
- The user device has enough memory available for installation and proper functioning of the application.

5. RESULT AND DISCUSSIONS

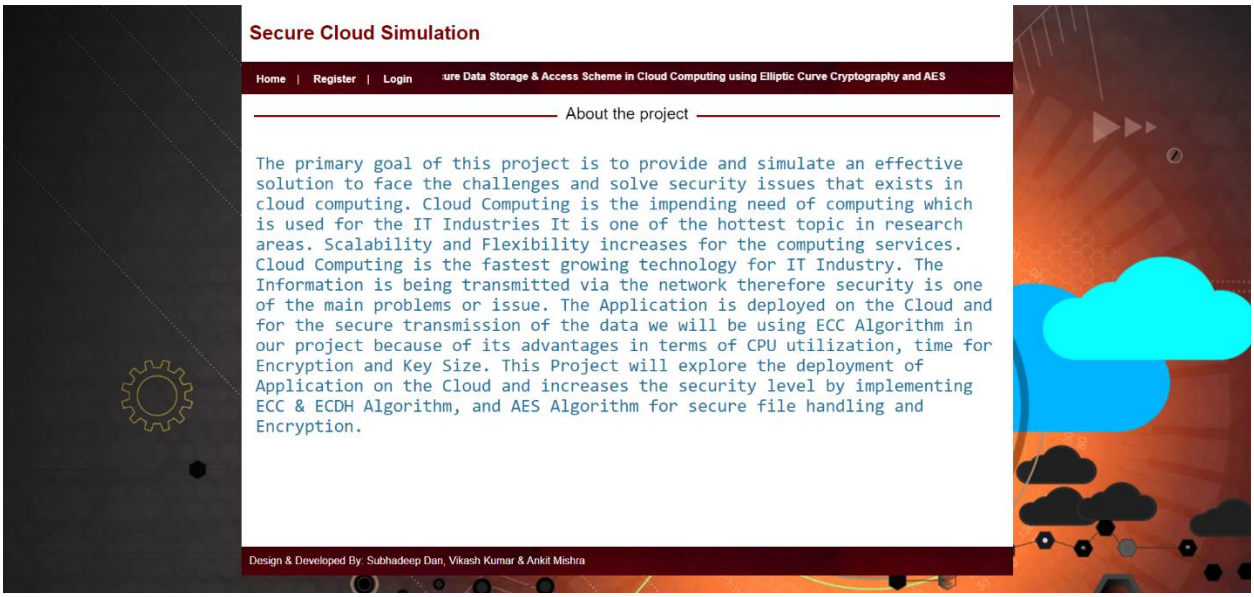


Fig. 11

This is the **landing page** of the web application – the very first page which is visible when the app is launched in the browser of the user's system. This page lets the user know about the application and let the user to choose between first time registration and login features. Along with this, the page contains tabs for download and upload section also. It contains, app logo, tag line and makes the user aware about the goal of the application is short period of time and enhances aesthetic value.

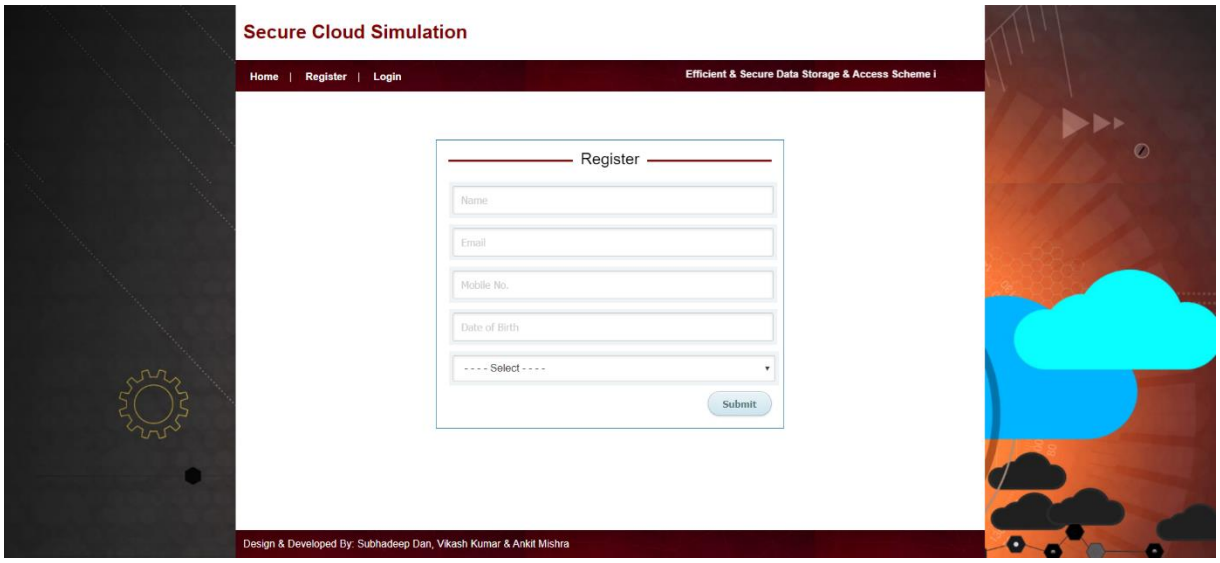


Fig. 12

This is the **Registration Page** of the application which is displayed when user is using the application for the first time or does not possess a user account.

The form here takes user's full name, email address, mobile number, DOB and gender as input to store user's information and validate the user before giving access to the app data. It first checks for all possible errors in the credentials on the client side itself using regular expressions and pattern matching. Later, if the data passes all the test cases, it is sent to server side to validate and store the details in the database to create a working profile of the user.

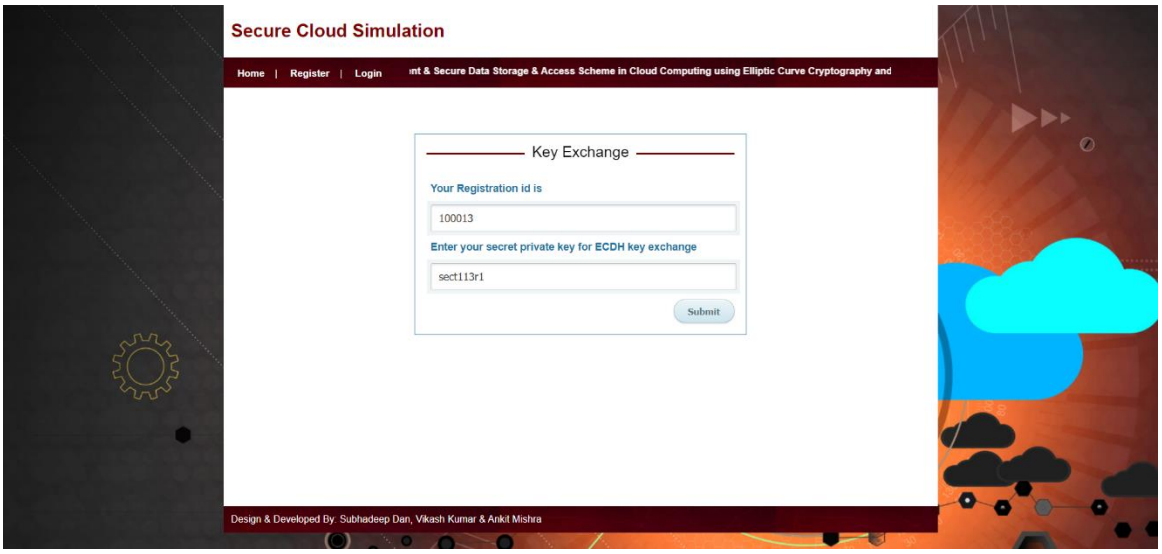


Fig. 13

This is the **Key Exchange** page of the application. Using ECC algorithm, public key and private key both are generated. Here Sender will be used to encrypt the data and receiver i.e. B is used to decrypt the data by using its own private key. The form here takes, registration number along with secret key for successful key exchange.

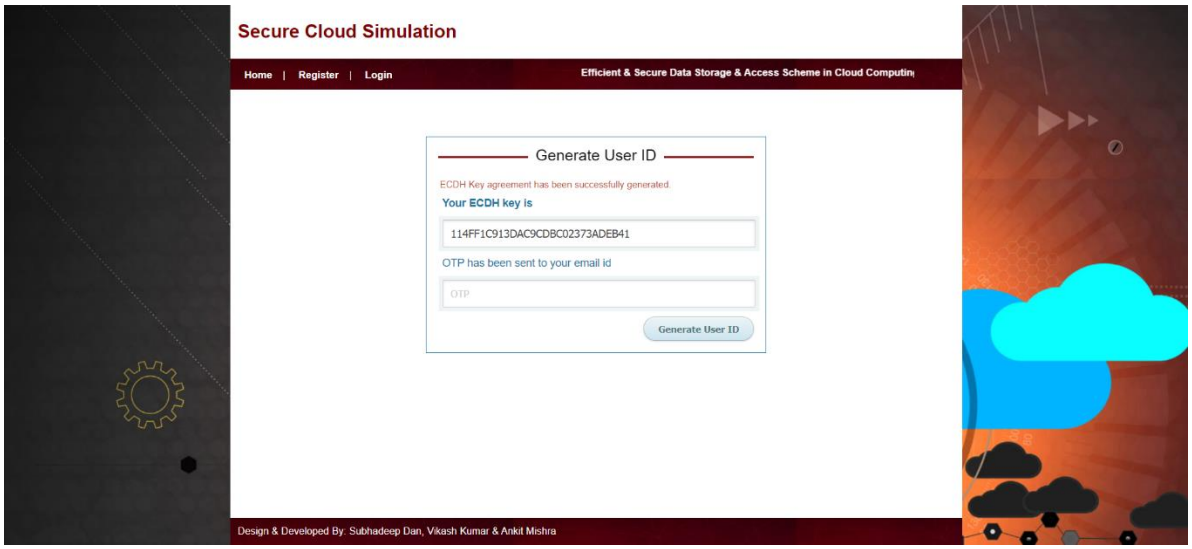


Fig. 14

This is the 3rd stage of Registration process itself. Here ECDH key agreement has been automatically generated successfully and **OTP (one time password)** is sent to the email address given by the user on stage one of the registration. The app takes OTP as input and after proper validation of both the fields, it passes the control to the next stage of new user registration.

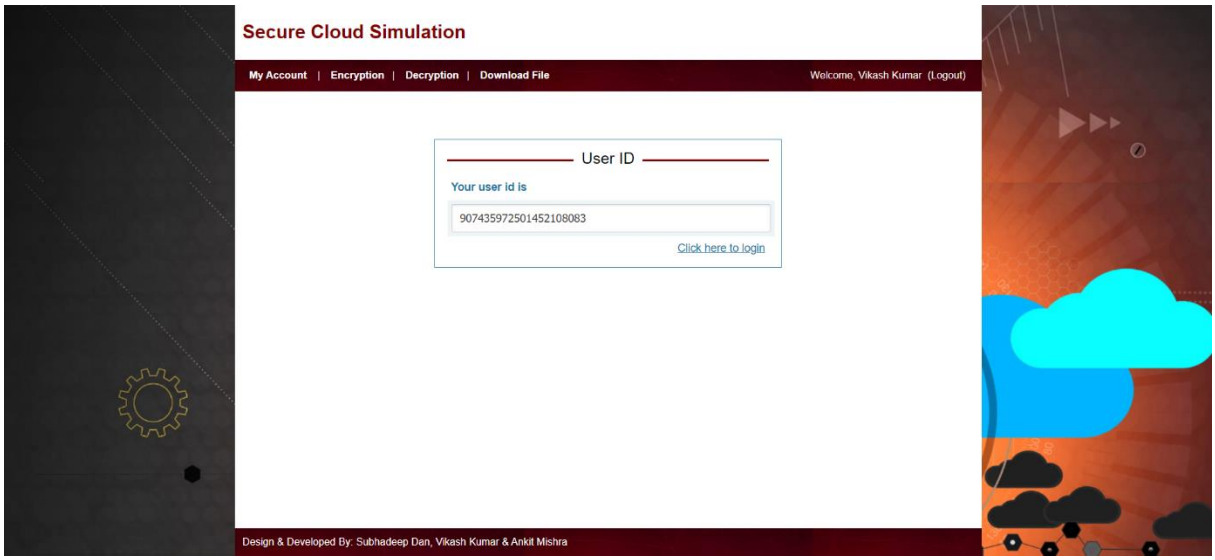


Fig. 15

On successful validation, the application generates a unique **User ID**. The user is requested to save this ID as, once the registration is done, the user will be using just the User ID generated here and the secret key entered earlier to use all the features and perform validation further in the application. The new user registration completes here and now the user can easily login to access his profile and use all the features of the application.

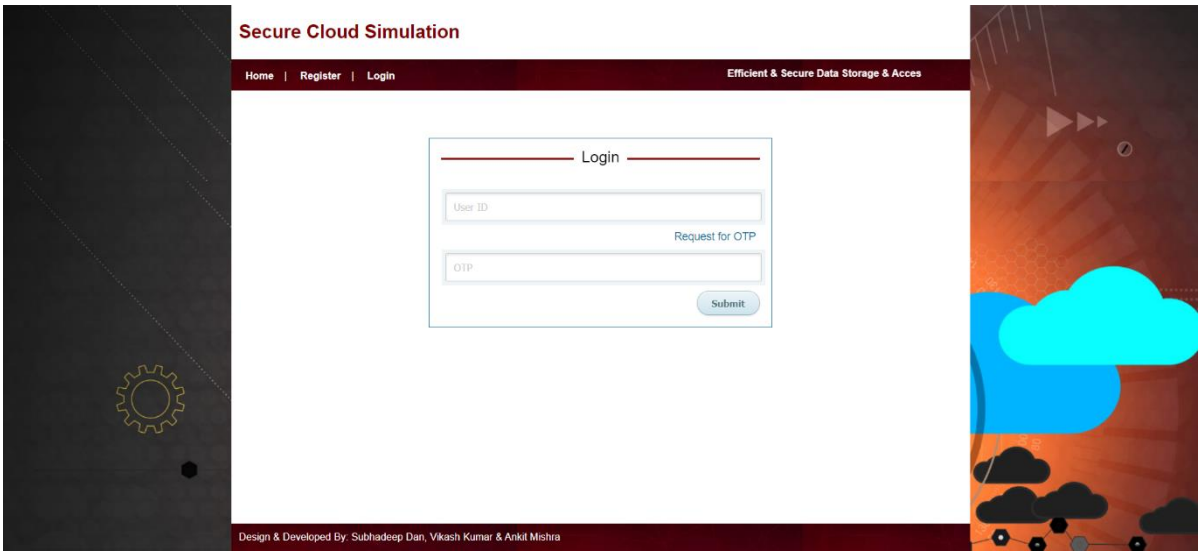


Fig. 16

This is the **Login page** of the application which is loaded when the user clicks on the login tab button. The page consists of a simple form which inputs the User ID of the user generated during registration process and the OTP which is immediately sent to the user's email address as soon as he clicks on 'Request for OTP' button in the form. Later, both the values in the fields are validated over the server with the values in the database and if successful the user is taken to the next page that is Dashboard of the application, else error is generated.

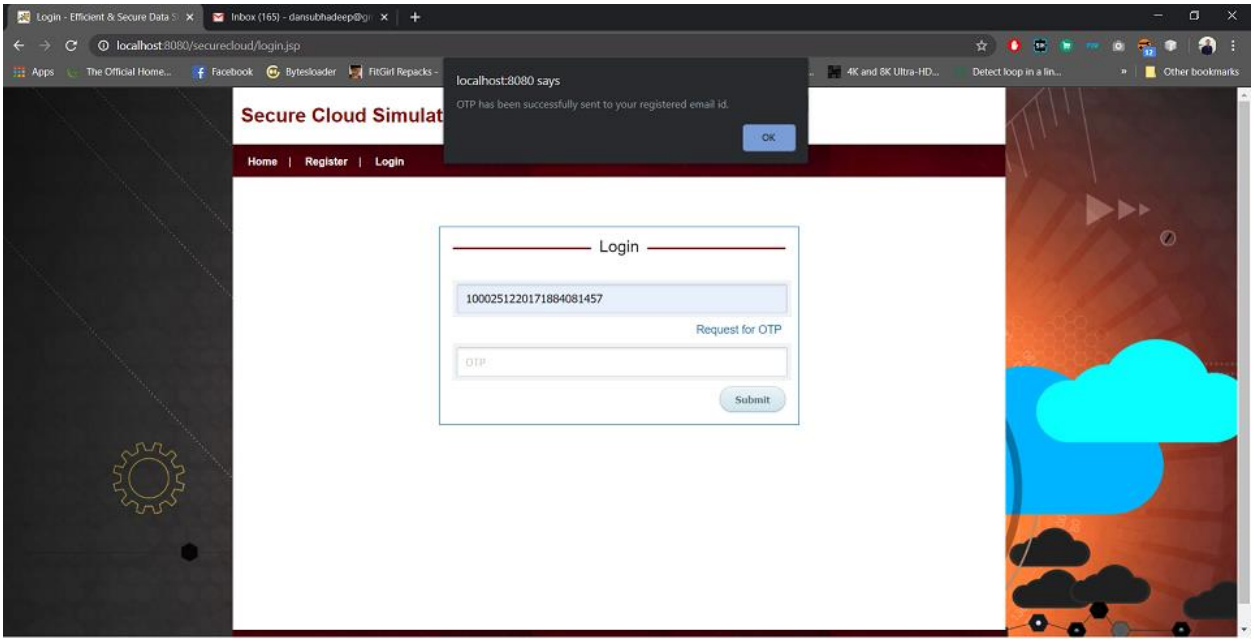


Fig. 17

Here a confirmation message is shown to verify that the OTP is successfully delivered to the registered email ID of the user.

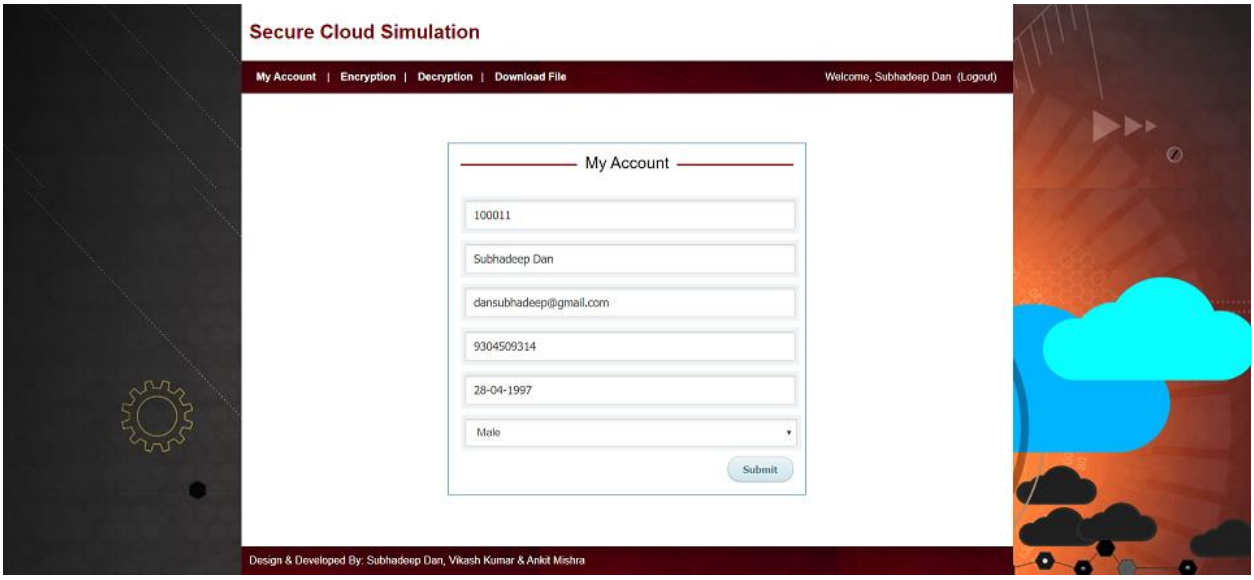


Fig. 18

This is the **Dashboard Page** of the application. When the user is able to successfully login into the app for the first time, he is taken to the My Account section where he is shown the current details of his account stored in the database and is given an opportunity to update any field if required and click on submit button to save. The dashboard page serves as a navigating page as from here the user can go-to encryption, decryption download and upload sections and can log out from the app if the work is done.

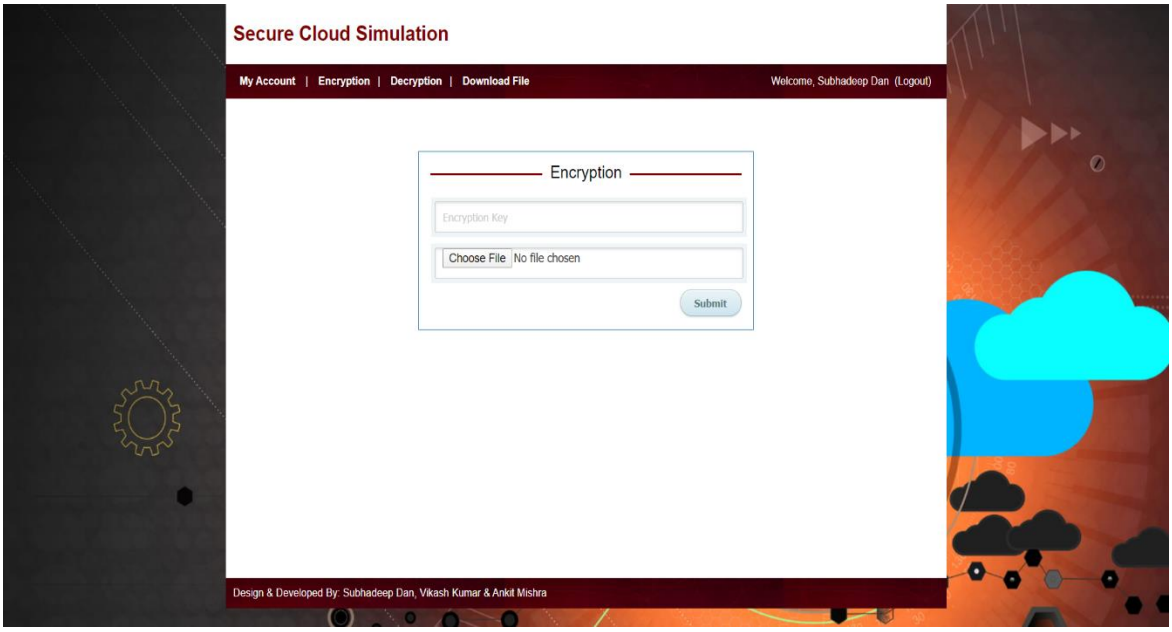


Fig. 19

This is the **File Encryption** page of the application. If the user wishes to upload a file in the cloud application and encrypt it to ensure security, he would hit the encryption tab. Next he is asked to enter the Encryption key which is actually the same secret key entered at the time of registration also. After that, he is asked to select the file to be uploaded from his local system on which the application is running. Lastly, click on submit to process the encryption and saving of file.

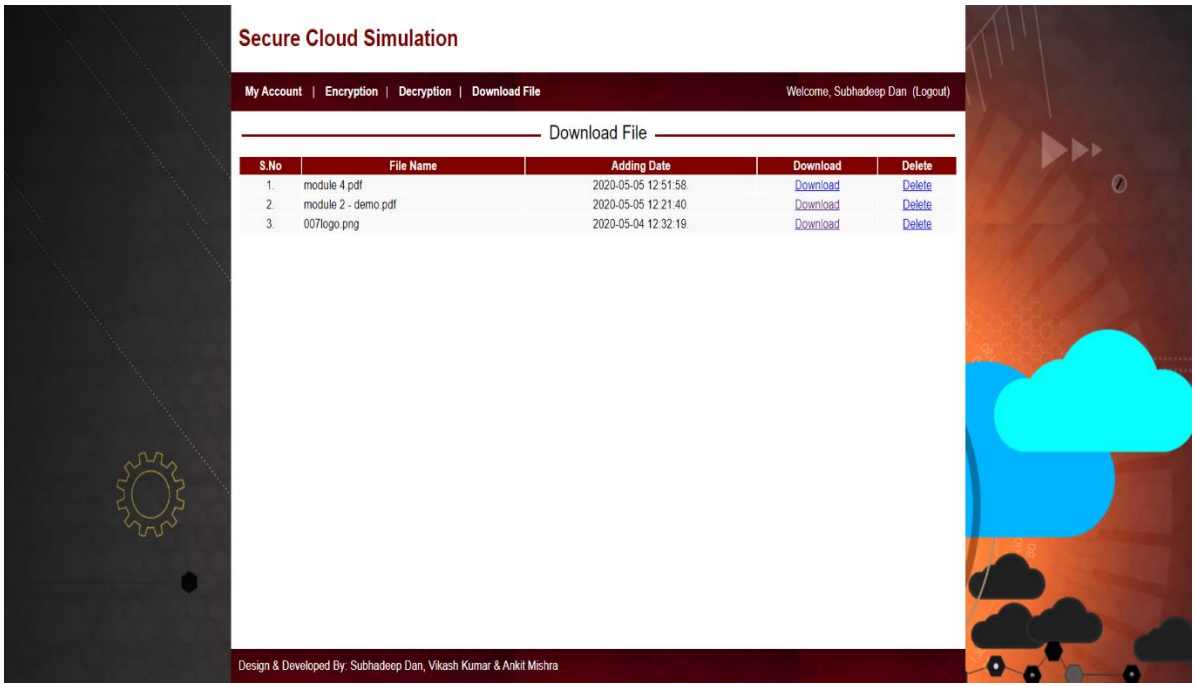


Fig. 20

This is the **Download File** Page of the application. Here the user can download the files which he/she has uploaded, but the file which will be downloaded would be encrypted using AES and cannot be opened without decrypting it. Hence, even if anyone gains access to this file, he/she will not be able to open the file thus maintaining file security. Only the owner can decrypt the file by going into the Decryption Page and entering the secret key provided during encryption.

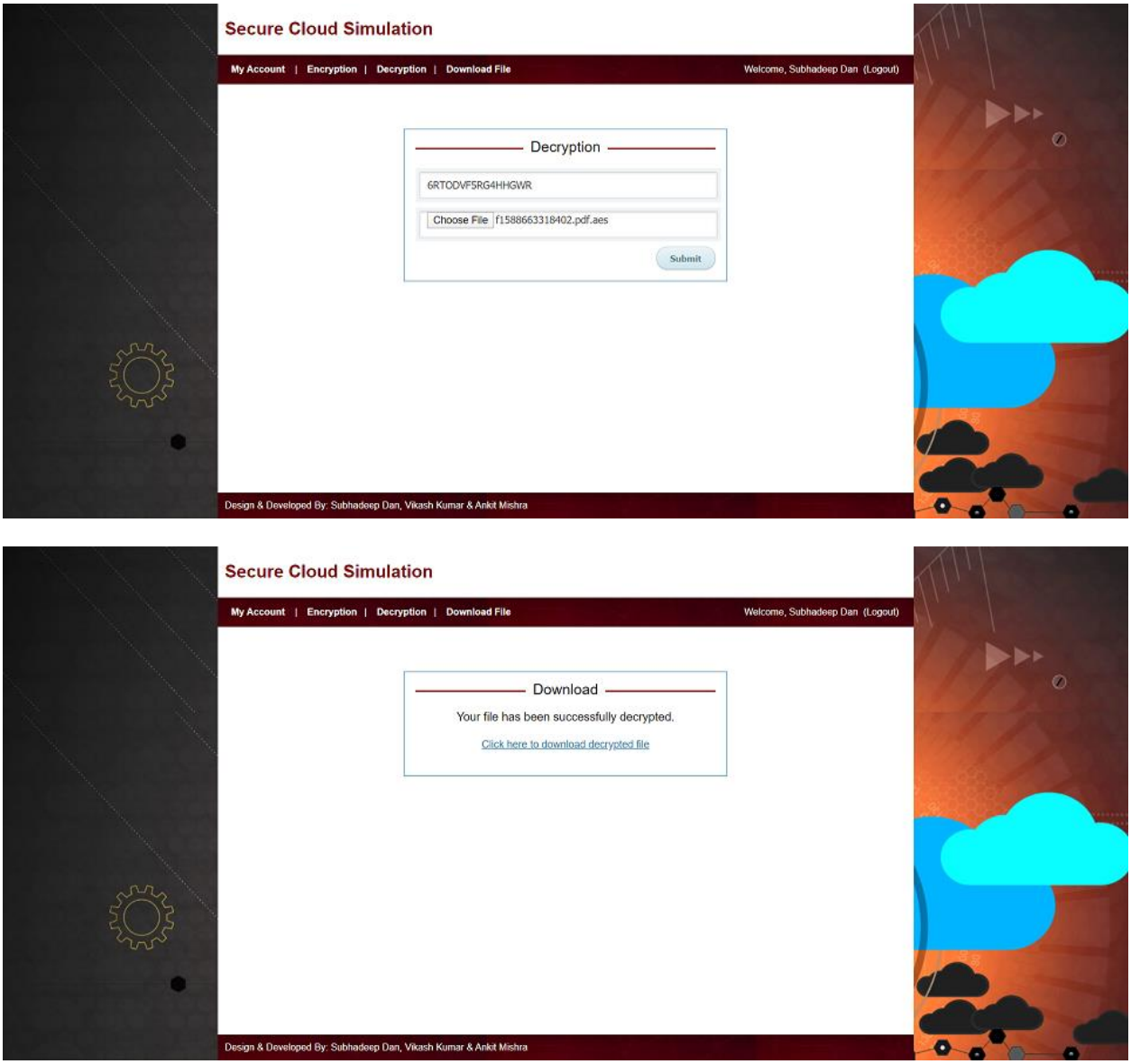


Fig. 21

This is the Decryption section of the user's account. Now after downloading the encrypted file, in order to decrypt the file, the user has to enter the respective AES key that was generated and given to him, and select the file to download. After this, the chosen file is decrypted and ready for download. The downloading would start as soon as the user hits the download button.

6. CONCLUSION AND FUTURE WORK

6.1 CONCLUSION

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 security techniques and efficient encryption algorithms to secure the file along with 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 client's own system. This application will allow users to upload file of different formats with security features including Encryption, secure OTP verification, uploading and downloading over the cloud securely.

This prototype works using 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 to 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 only by the user of the data, no one can decrypt the data, even though the hacker can get the data through some approaches.

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.

6.2 SCOPE FOR FUTURE WORK

The development of this project surely prompts many new areas of investigation. We have successfully completed all the phase of the development and did our research prior to the development about the various encryption techniques along with their strengths and weaknesses. After in depth comparisons and review we decided to use ECDH and AES Algorithms to implement the whole idea of this model. We referred multiple research papers whose links can be found in the references. Lastly, we implemented the model using Java Servlets & JSPs, Apache Tomcat server and MySQL for storage. We will be using cloud hosting services for the actual deployment of the project. For the GUI, we have used HTML and CSS 3.

In the last semester, we completed database modelling, new user registration module, secure key generation, exchange module along with introduction, user interface of the application and we managed to develop approximately 50% of the whole project. In current semester, we have worked on modules like, file encryption-decryption, secure file download and upload using user ID and another OTP, Secure AES Key generation for the file handling features, testing of the whole application, load balancing, checking the border cases to make sure that all the modules are completed and running.

Keeping all the deadlines in mind and the project development life-cycle of our project, we have been able to complete all the phases of the development cycle on time with minimum possible errors. Talking about scope of future work, we believe that it is possible to minimize the processing time taken in all the encryption-decryption processes by using professional hosting services and even better implementation of the security model. Also, some advanced hybrid cryptography algorithms and system can be incorporated to ensure cutting edge security and protection.

6.3 REFERENCES

1. Dr. K N Mishra, "A Novel Mechanism for Cloud Data Management in Distributed Environment. Data Intensive computing Applications for Big Data", IOS Press,2018.
2. 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).
3. 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).
4. 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.
5. Xiang Tana, Bo Aib"The Issues of Cloud Computing Security in High-speed Railway "in 2011.
6. 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.
7. Eman M.Mohamed and Sherif EI-Etriby "Randomness Testing of Modem Encryption Techniques in Cloud Environment" in year 2008.