Chapter 5

MULTIFACTOR AUTHENTICATION IN CLOUD COMPUTING

5.1. Introduction

Authentication is a key procedure for ensuring the security of information. To improve the authentication in the cloud computing, a lot of research has been done. Remote authentication is a method commonly used to determine the identity of a remote client. In this chapter, we proposed an effective method for authenticating clients, namely: the use of password, OTP and access control based on biometric data. The proposed system includes user identification / password, biometric functions and a mobile phone for generating a unique password.

A multifactor authentication method uses more than one factor, so it is not easy to do it than single-factor authentication. Therefore, correctly developed and applied methods of multifactor authentication are more reliable and stronger limitations of fraud [126].

Existing authentication methodologies involve three basic factors:

- Something the user ***knows*** (e.g., password, PIN);
- Something the user has (e.g., ATM card, smart card)

Something the user is (e.g., biometric characteristic, such as a fingerprint).

5.2. Traditional Authentication Techniques

The combined user authentication method and password is a method that is often used for authentication, but can be hacked using existing hacker tools [127]. OTP means "Password once." In the OTP method, a password is provided upon request. OTP can disrupt the possibility of theft and re-use of the password. The assigned password is only valid for a login session or a transaction timeout and can only be used once. The most important error solved by OTP is that, compared to static passwords, they are not vulnerable to repeated attacks. These systems are not

cheap and reliable to protect the system. Users of OTP-systems are still sensitive to the type of attack in the system known as the attacks of people in the middle [131].

5.3. Common Multi-Factor Authentication Methods

5.3.1. Biometric Authentication

Biometric security mechanisms acquire biometric data from an individual, extract a set of characteristics from the data, compare established functions with sets of functions stored in the database, and perform an action based on the result of the comparison [128]. Identification became complicated in a highly interconnected cloud network. The need for an agreed method based on cloud security has increased as a result of greater concern for security.

Biometric recognition is a reliable and adequate methodology for identifying people based on their biometric characteristics. It can be defined as an automated methodology that makes it possible to uniquely identify people using their physiological or behavioral characteristics [129]. The introduction of biometric recognition requires serious protection of confidentiality from possible misuse, loss or theft of biometric data. Existing biometric identification methods and methodologies that preserve confidentiality are based primarily on conventional cryptographic primitives, such as homomorphism encryption and unconscious transmission. These primitives inevitably bring enormous cost to the system and are not applicable to large-scale practical applications [130]. Data leaks and security leaks may be caused by inadequate authentication [131]. Cloud services are paid services, so identifying an authorized user is a serious problem in cloud computing.

At present, biometrics is the security system most used in various organizations, academics and different societies. This helps overcome many of the disadvantages of the authentication methods mentioned above. To solve the problem of authentication in cloud computing, there are various traditional methods, as indicated below, but they bring a lot of inconvenience.

5.3.2. SMS-Based One-Time Multi-Factor Authentication

This type of authentication technology uses mobile phones as a relatively inexpensive factor. During registration in the system, the user provides his mobile phone number so that they can be provided with an additional one-time password with a limited term or PIN when they want to log in or authenticate their credentials [131]. During the logon process, they provide the

user ID and password. They request an authentication server to send them OTP to their pre-registered mobile phone to complete the authentication process. The advantage of this technology is that it uses the second factor and minimizes the cost [132].

5.3.3. Software-Based (Certificate) Authentication

This scheme is less preferable for multifactor authentication methods. They do not provide one of the factors, regardless of the computer from which the user accesses the resource, which requires multifactor authentication. It can be easily copied or stolen.

5.3.4. Internet Protocol Address (IPA) Location and Geo Location

In this structure, users can recognize their geographic location. For example, if a user has made his transactions in the country, it is assumed that their next transactions will be conducted only in that country. Tokens generate a random number used together with a PIN or password. Smart cards are delivered to the reader. Then they are unlocked using a one-time PIN or password, limited time codes sent by SMS [133].

5.4. Problem Statement

We originate two difficult problems related to security during the survey. First, security from the inside; It is assumed that the initiator can access the first level authentication credentials. This is unacceptable, so multi-level authentication is mandatory. Secondly, access control; data is on the cloud side under the supervision of an external cloud service provider. Then there must be some mechanism for authenticating the user on the client side.

5.5. Multifactor Authentication Mechanism for Access Control In Cloud Computing

In In proposed work, we have utilized the following authentication methods to design strong access control mechanism for cloud computing.

- PIN/Password
- Biometrics
- SMS based mobile OTP

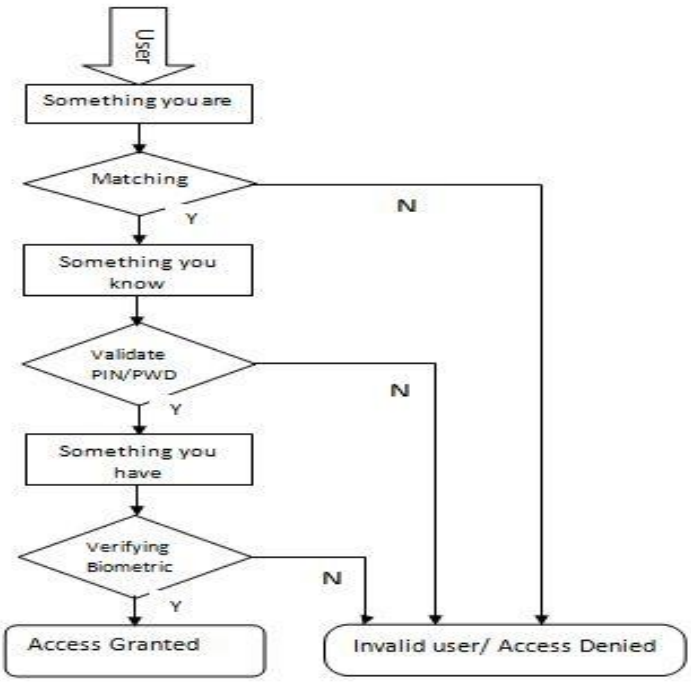

Figure 5.1: Multifactor Authentication Overview

5.5.1. Biometrics

Biometric refers to the study of measurable biological characteristics. Regarding computer security, biometrics refers to authentication methods that are based on measured physical characteristics that can be automatically verified. There are several types of biometric identification schemes:

5.5.1.1. Fingerprint Recognition

Fingerprint is a drawing of the crests and valleys on the surface of the fingertip, the formation of which is determined during the first seven months of development of the fetus. It was empirically determined that the prints of the twin prints are different [134]. Fingerprint recognition refers to an automated method of checking the correspondence between two human prints. Dry fingers, dirty fingers can affect the system and can show an error. The problem with large-scale fingerprint recognition systems is that they require a lot of computing resources. Finally, the fingerprints of a small proportion of the population may be unstable for automatic identification due to the aging of genetic factors. A professional reason, similar to manual work,

can have a large number of cuts and bruises in their fingerprints that are constantly changing [135].

5.5.1.2. Voice Recognition

Voice is a combination of different physiological or behavioural biometric characteristics. The physiological features of an individual's voice are based on their shape and size of appendages (vocal tracts, mouth structure and cavities of nasal and lips) [135]. Voice recognition is used to authenticate user's identity based on patterns of voice pitch and speech style. However a user's voice can be easily recorded and may use by unauthorized user. A disadvantage of voice based recognition is that human's speech features are very sensitive to a number of factors such as noise and voice signal quality is typically degraded in the quality by the communication channel.

5.5.1.3. Signature Recognition

Signature recognition is used to authenticate a user's identity based on the characteristics of their unique signature. This is the biometrics of behaviour that changes over a period of time. It is influenced by the physical and emotional conditions of the signatures.

5.5.1.4. Retinal Recognition

Recognition of the retina is the recognition of people following the pattern of the retinal blood vessels. However, this is a very intrusive and expensive technique.

5.5.1.5. Iris Recognition

Iris recognition is a method of identifying people based on unique patterns in the annular region that surrounds the pupil of the eye. The accuracy and speed of the realized diaphragm recognition system are compatible and allow the implementation of large-scale identification systems based on information on the iris. Iris recognition systems have a very low false acceptance rate (FAR), and the false rejection rate (FRR) of the system can be high compared to other biometric characteristics, such as fingerprints, voice, retina and face [136].

5.5.1.6. Palm Recognition

The recognition of the palm is based on ridges, main lines and wrinkles on the palm surface. This method is very expensive and not suitable for children, as the palm lines change

when they are fully grown. All the above methods, as a rule, tell us that none of them is feasible because of its various shortcomings [136].

5.5.1.7. Face Recognition

It is non-intrusive methodology and facial attributes are probably the most common biometric feature used by humans to recognize one other [137]. In order that a facial recognition system works well in practice as follows:

- **Face Detection:** It should automatically detect whether a face is present in the acquired image.
- **Face Location:** To locate the face if there is in the used face database.
- **Recognition of Face:** To recognize the face from a general viewpoint from any posture/profile.

This chapter demonstrates a new proposed "biometric system" on the security issues of cloud computing.

5.5.2. Biometrics for Cloud Security

A biometric system is essentially a system based on pattern recognition. Gets biometric data from an individual, extracts a set of important characteristics from the data, compares established characteristics with sets of functions stored in the database, and performs an action based on the result of the comparison. Biometric identifiers or signs are classified as physiological characteristics in comparison with behavioural characteristics [135].

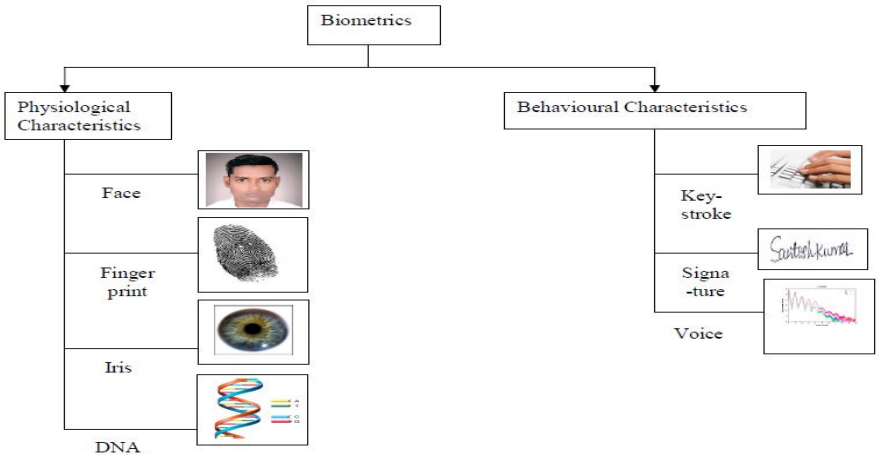

Figure 5.2: Biometric Characteristics: Physiological Characteristics and Behavioural Characteristics

Physiological characteristics: face recognition, fingerprint, finger sensation, iris recognition, arm geometry, DNA, retina and ear recognition. The behavioural characteristics associated with human behaviour, including the rhythm of typing, walking and voice [137]. By using biometric data, you can set an identifier based on:

- Who you are, not what you have, for example, an identity card or
- What do you remember, how to password.

5.6. Mode of Operation of Biometric System

Depending on the application context, biometrics system may operate either in the verification or identification mode.

5.6.1. Verification Mode

In the verification mode, the subject confirms the identity, and this input image is compared with the data of the claimed identity through their respective sets of characteristics to confirm the claim. This is a method of positive recognition, where the main goal is to avoid having several subjects use the same person [138].

5.6.2. Identification Mode

Identification is a critical component in the application of negative recognition. The main area of negative recognition is preventing one person from using one person [139]. A biometric system can be demonstrated as a characteristic pattern recognition system, where the image of the input subject is reduced to a set of features that are subsequently used to compare them with the sets of functions of other images to determine their identity [140].

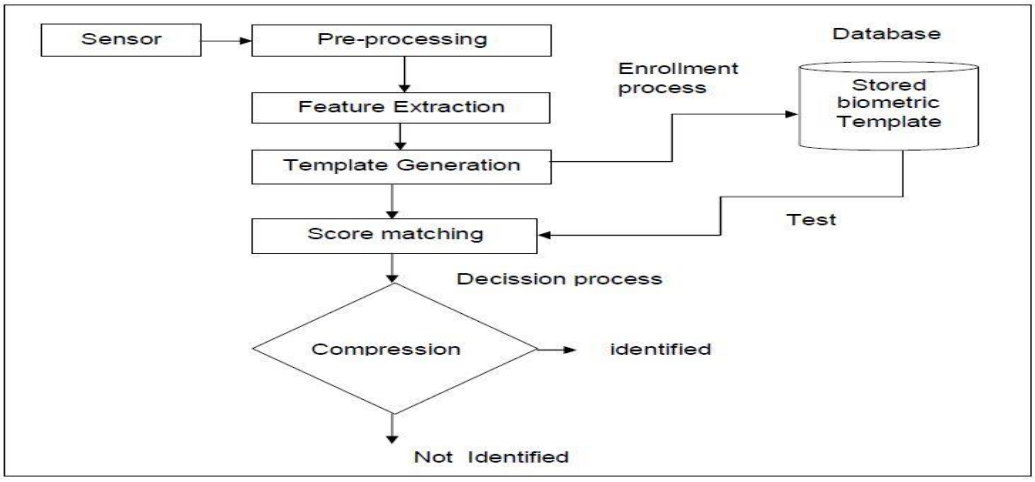

Figure 5.3: Block Diagram of a General Biometrics Recognition System

A biometric recognition system can be achieved with images of individuals who were completed during the acquisition phase. The main stages of the classical general biometric recognition system are illustrated in figure 5.3.

5.7. Components of Biometric System

A common biometrics system can be validated as having four main modules:

5.7.1. Sensor module

A biometric system requires a suitable biometric reader or scanner to collect common biometric data of people. For example, images of fingerprints, an optical fingerprint sensor (minutiae) can be used to capture friction, the shape of the crest and the size of an individual fingerprint [141].

5.7.2. Pre-processing

The related biometric pre-processing technologies, including: image noise removal, edge sharpness, image restoration, image segmentation, drawing extraction and declassification, etc. [140]. Some pre-processing stages include noise filtering (for example, with Gaussian windows [141] and re-sampling.) Re-sampling is performed on some systems to obtain a representation based on methods, it consists of equidistant points, avoids the resampling step, because some Discriminatory speed characteristics are lost in the process [142].

5.7.3. Feature Extraction

The method of extracting characteristics determines the quality and suitability of the biometric data obtained by the sensor in the estimates [142]. The received data obey the algorithm of signal improvement to improve its quality. To facilitate comparison or comparison of the original digital representation, it is usually handled additionally using a feature extractor to create a compact but expressive representation called a set of functions. For example, the position and orientation of the small points in the fingerprint image will be calculated in the feature extraction module.

5.7.4. Matching Process

The extracted characteristics should be compared with the data stored in the database (template database) in order to establish the identity of the biometric input characteristics. In its

simplest form, matching involves creating a conformity assessment by comparing sets of functions corresponding to two images. The score of the match indicates the similarity between the two images [142].

5.7.5. Decision Process

At the decision-making stage, the corresponding estimates generated in the corresponding module are used to make the final decision. In the identification operation mode, the result is a list of possible matching identities ordered by their coincidence [142].

5.8. Implementation of Biometric System for Cloud Security

This research usage a generic biometric methodology which provides the security to cloud [142]. The framework consists of following parts which are illustrated in figure 5.4**:**

5.8.1. Stage I: New User Registration

User or consumer must first register with the cloud server if users / consumers want to access cloud resources. To register to the server in the cloud, perform the following steps [142].

- People (User / Consumer) must complete the registration form provided by the cloud service provider. It contains detailed information about the user.
- People (User / Consumer) must provide an identifier. E-mail valid as a biometric user name during registration.
- The Biometrics system checks the e-mail ID based on the availability of this user name. The user name must not be repeated or be the same as the user name.
- After checking the availability of the user name, you must create a password. Individual image through a webcam or high-resolution camera is stored in the database as a password.
- After providing the correct user name and saving the image as a password, registration is completed on the cloud computing server**.**

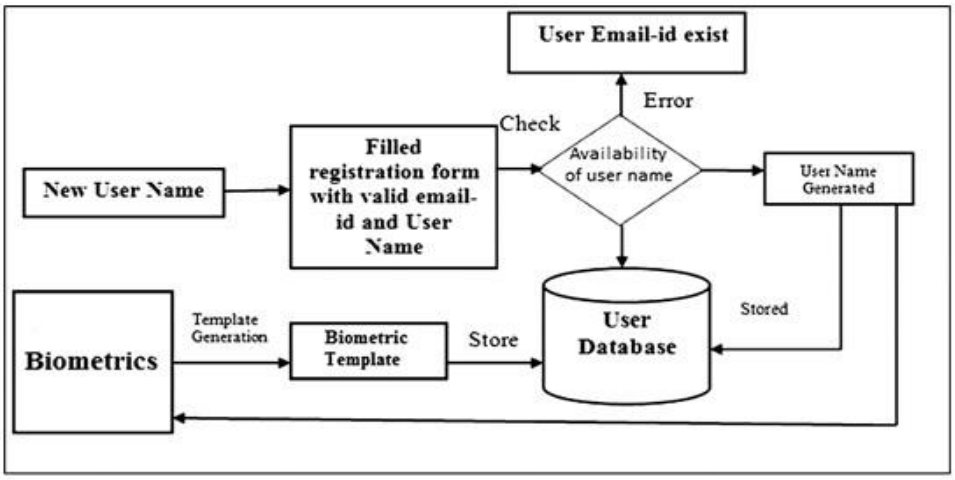

Figure 5.4: New User Registration in Cloud Using Generic Biometric System

5.8.2. Stage II: Assignment of User-Id and Password

This stage provides a form of communication between the user and the network in the cloud when the registered user wants to access resources on the cloud server. The registered user must then log on to the cloud server [142]. Below are the steps to enter the cloud server:

- People (user / consumer) must enter a valid user name in their login interface, which was already provided by the user at the time of registration. And for the password, the user's image is captured by a web camera or a high-resolution camera.
- The biometric system verifies the user's name and the user's biometric functions (for example, the image) as a password provided by people.
- After associating a user name with a user image as a password, the biometric system provides access to the cloud services for the user. If the user name or biometric functions of the user (for example, the image) do not match, an error message is displayed in the biometric system. The following figure 5.5 depicts the complete working steps.

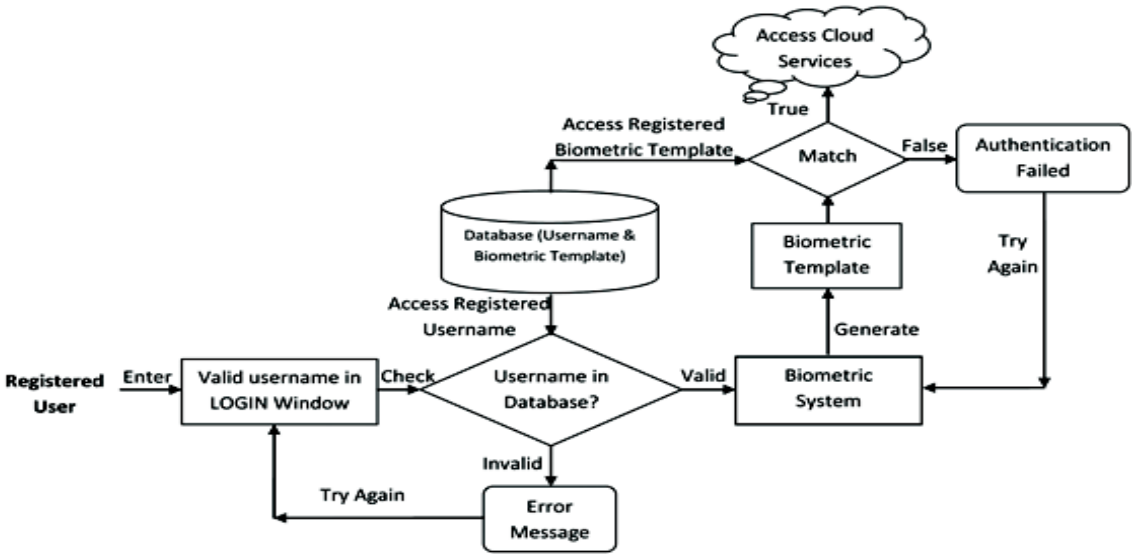

Figure 5.5: Registered User Registration in Cloud Using Generic Biometrics Recognition System

5.9. Out of Band Authentication

Commercial institutions and other organizations that require high security implemented this type of authentication. To gain access, there are two separate and independent authentication channels that must be compromised for an attacker [143] using this authentication scheme. An additional method is that users can make a phone call from a registered number or answer a phone call automatically created by the institution. Another method is to ask the user to send text to the code that is displayed after logging in from their smartphone registered in the institution.

5.9.1. Steps to Generating OTP

Assume the following system parameters:

i. Username = z92A
ii. PIN = 1984
iii. IMEI = 6876543210123453
iv. IMSI = 123456789123456
v. Time of Generation = 11/11/2013 11:02 AM

Step-1 the user wishes to login into a secure website.

Step-2 the user sends an encrypted SMS to server.

Step-3 the server received the encrypted SMS.

Step-4 the server decrypts and breaks the SMS into certain parts: Sender's Mobile Number, Username, PIN and IMEI number.

Step-5 Server checks the information against the database to ensure that user is genuine, if user is not genuine then server ignore the SMS.

Step-6 If the user is genuine then server generate a OTP and this OTP is encrypted by a Unique symmetric key shared between server and user.

Step-7 server sends the encrypted OTP to user via SMS.

5.9.2. The OTP Server and Authentication Protocol

The secret key and the security are the two main constraints on which OTP safety is based. OTP cannot produce the same code twice and cannot return to the original code. Even if a hacker intercepts a lot of OTP, an attacker cannot learn the algorithm, which means that even if he knows the key, he cannot return to the counter that OTP generates. Then, without a key and counter, it is impossible to find a template, even with millions of OTP, to guess the key and the value of the current counter [144].

OTPs are typically used to authenticate or verify a transaction using a credit card. In the case of a transaction, OTP is sent to the user's mobile phone. For authentication, you can use a secure token or request to send OTP to the user's phone / e-mail [145].

5.10. Method For New User Registration in Cloud

There are several steps to register with any cloud service provider. There are several steps to register with any cloud service provider.

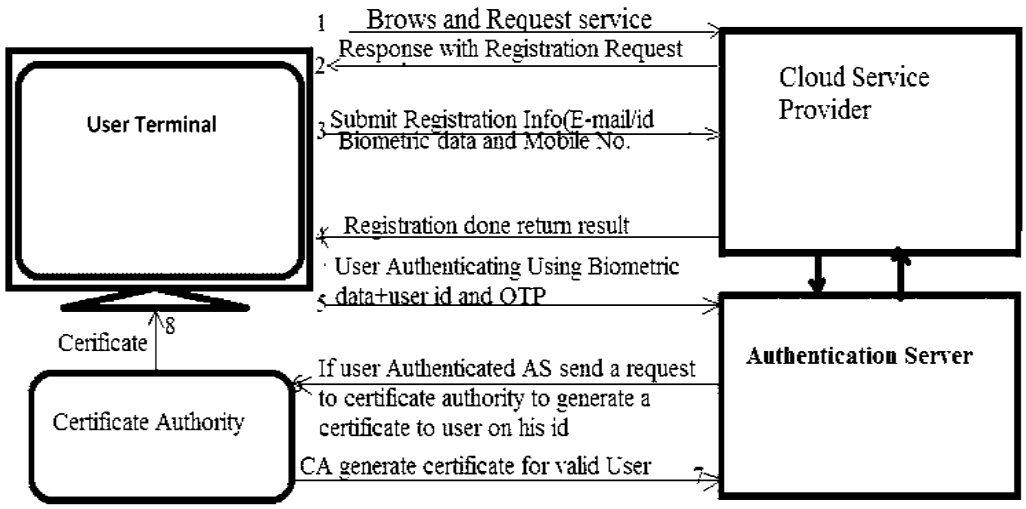

Figure 5.6: New User Registration in Cloud

Step1- User brows and sends request to CSP.

Step2- CSP receives his request and sends him a registration form to user.

Step3- User provides his personal information like name, address, mobile number and biometric characteristics like fingerprint also first time to get registered with CSP. This information of user is kept by Authentication Server.

Step4- now user is registered by providing information in step3

Step5- after successful registration in step-4, the user provides his biometrics data and OTP to authentication server to authenticate first time with AS.

Step6- after successful authenticated by authentication server in step-5, the AS sends a request to certificate authority to generate a certificate to user.

Step7- the certificate authority generates a certificate to user.

Step8- CA sends its copy to AS and user e-mail id also.

The user is registered and authenticated after multiple steps by the authentication server and then user avails the specific services of cloud.

5.11. Proposed Method For Access Services From A Cloud Service Provider

In this section we have presented our proposed model architecture as shown in figure 5.7. The architecture works in several steps as given below

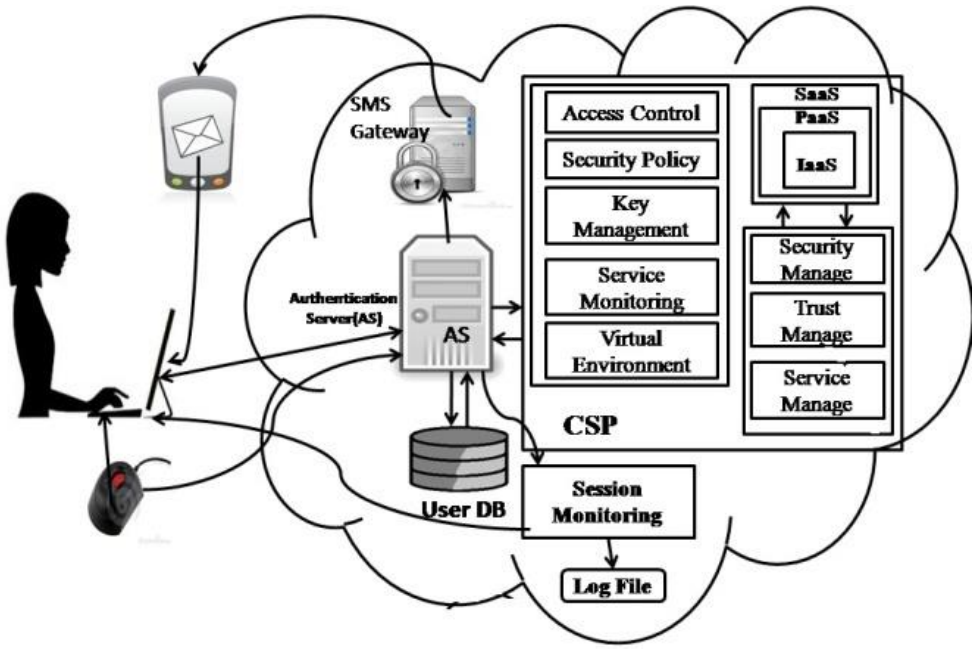

Figure-5.7: Multi- Factor Authentication Scheme for Access Control

After successful registration the user can get the services from specific cloud service provider after successful authorization by AS. There are several steps to get the service from CSP:

Step-1 the user opens the URL of the CSP and enters his credentials.

Step-2 if user id=true (matched from already submitted credentials in user database)

then provide biometric-data;

else access denied;

if biometric-data=match; (a onetime password send to user's registered mobile no.)

then provide OTP;

else access denied;

if OTP=verified;

then go to next step;

Step-3 A certificate issued to user and he presents it to session monitor

If certificate=correct;

then user permitted to access the service;

else user is invalid;

On every access of the services, session monitoring creates a log file for audit purpose in future.

5.12. Security Analysis

The proposed framework confirms several limitations to increase the security as follows:

5.12.1. Robust Security

The framework contains multiple factors to authenticate an individual so the possibility of a security breach can be significantly reduced as the hacker would not be able to access any information of the client/user.

5.12.2. Consumer Privacy

The proposed system keeps the user information in encrypted message. The messages are transmitted over a public channel. These messages cannot be decoded easily to get ID, PW etc. Hence, the scheme provides user privacy.

5.12.3. Mutual Authentication

At the eighth stage of the registration process, the user provides a certificate generated by the CA to the authentication server and the server authenticates it, and in the third authentication step, the session monitor checks the integrity of the server certificate. Therefore, the server checks the user. Therefore, mutual authentication is achieved.

5.12.4. Replay Attack

OTP is only valid for a login session and a key provided to the user via a mobile or electronic channel. In addition, the system provides a key session agreement between the user and the server, which also acts for a single sign-on session. Therefore, our scheme is strong against re-attack.

5.12.5. Password Guessing Attack

The method uses OTP, which offers great power for the circuit. Therefore, without knowing the OTP and the password generated by the user (using the hashing algorithm), this scheme cannot be decrypted using a password guessing attack.

5.12.6. Insider Attack

In this scheme, the password is digested with the SHA1 hash function and is never used openly, which is very difficult to break. In addition, attackers need a user password, OTP, and a user's biometric template to access the cloud. Only the current user can provide this information at the same time. Hence, the scheme is strong against insider attack.

5.13. Important Observations

- Our approach uses the concept of PIN / PWD, biometric functions and OTP for user authentication. Our model uses a complex password using a one-way hash function. The circuit also uses a one-time OTP in the next step, which provides more value for the circuit. Then, without knowing the secret user number, the server's secret and OTP, it's impossible to disguise it.
- The scheme proposed in is susceptible to server spoofing, since it provides client authentication instead of mutual authentication, which it does.
- Our model provides mutual authentication. At the eighth step of our model, during the registration in the cloud, the user provides a certificate generated by the CA to the authentication server, and the server authenticates it. Although in the third authentication step, the session monitor verifies the integrity of the authentication server certificate. Thus, the server checks the user.
- In [146], specify two authentication passwords based on identifiers, where users verify the use of smart cards, passwords and fingerprints. This scheme is vulnerable to passive listening. An attacker can successfully log in to the server on behalf of any claim identifier after passively listening to the legitimate login.
- Although the password in our proposed scheme is a hash, the schema never transmits the user's personal data in text format; Instead, it is digested with the SHA1 hash function, which is very difficult to break. OTP provides the strength of our scheme.
- In [147], a protocol is proposed that uses biometric data. In this scheme, the authentication server does not have the biometric information of registered clients.
- In our schema, the server maintains a database for storing the biometric information of all users through an authentication server in the cloud.

- In [148], several methods are presented for associating a cryptographic key with a biometric template of a user stored in a database. A cryptographic key cannot be detected without successful biometric authentication. However, a biometric database can compromise a client's privacy.
- Although our proposed scheme never transmits the user's personal data in text format. Messages are transmitted through a public channel. Obviously, these messages cannot be easily decoded to get ID, PW, etc. So the scheme provides privacy for the user.
- The scheme proposed in [149] explains another authentication scheme for the remote client based on biometric data using a smart card and password.
- Although our proposed scheme uses the ID / PWD concept, biometric characteristics and OTP, which ensure the strength of our scheme.

5.14. Implementation

5.14.1. Server Side

1. **Registration** – During server side registration the user have to provides his personal information. After successful registration process the user is to login for nest steps. The figure 5.8 is the screen shot of the registration page in implementation.

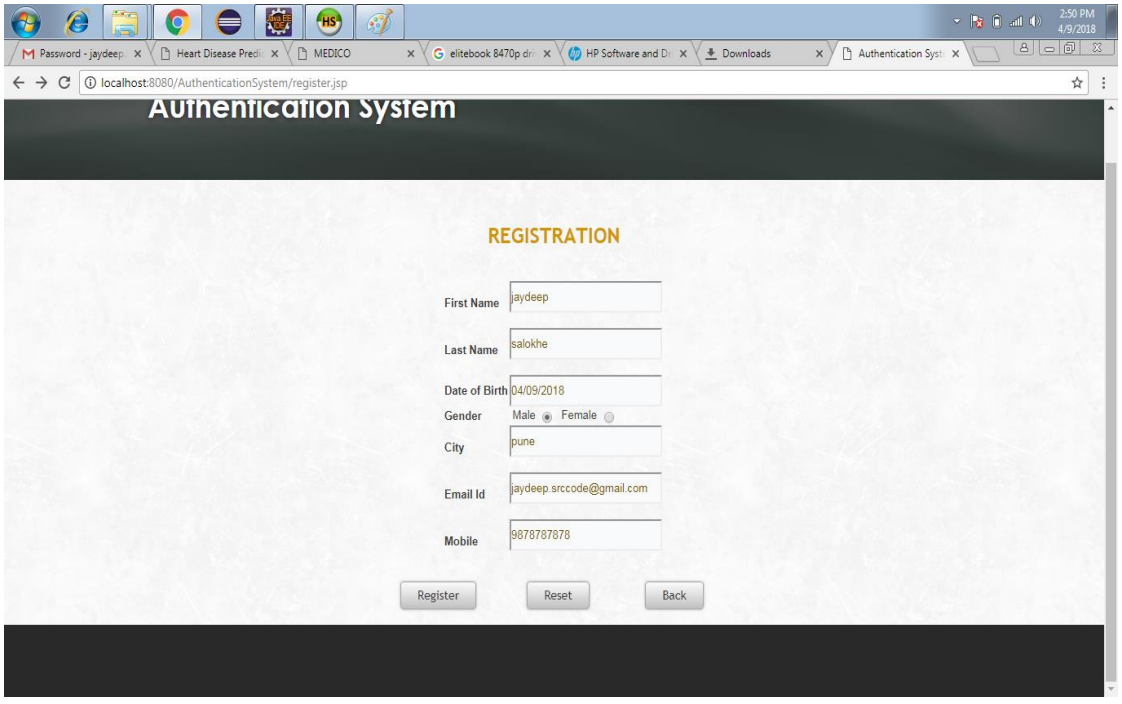

Figure 5.8: Server Side Registration

2. **Login** –After successful registration in server the user can login and request to services by entering username and password. The figure 5.9 depicts the screen shot of the login page. During the registered user enter his user id and the server validate his id from its database and then send an otp (password) to his registered email id.

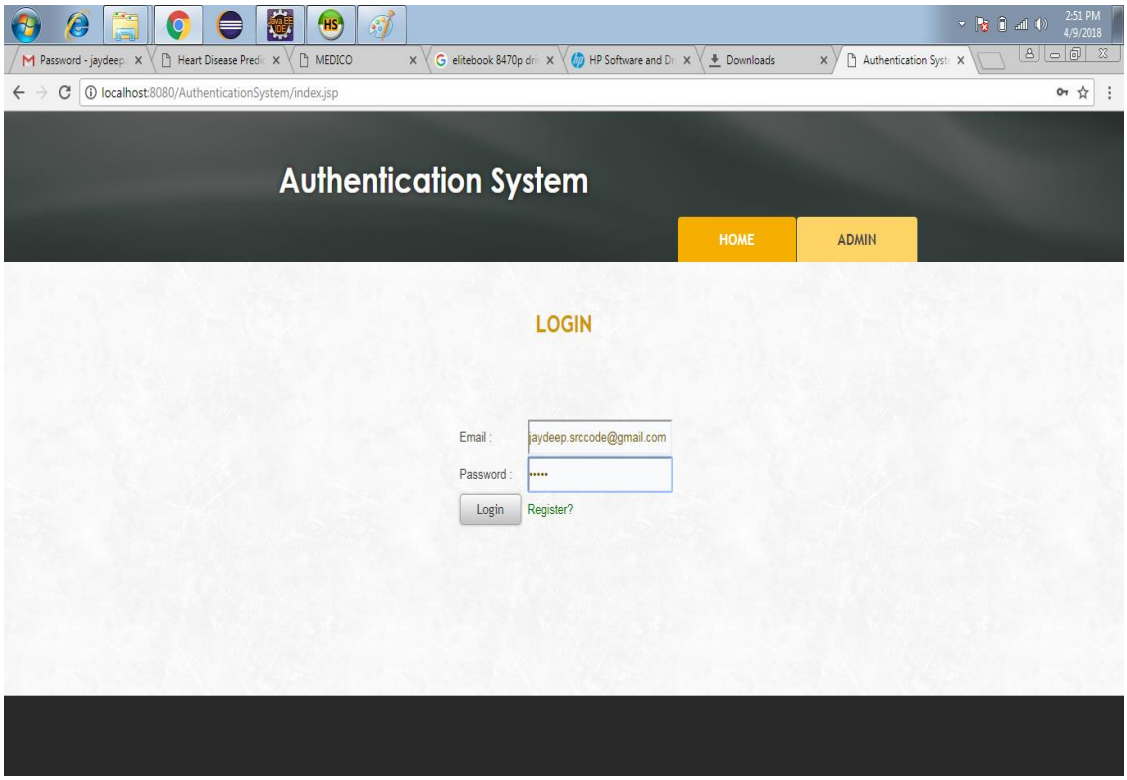

Figure 5.9: Login

3. **OTP as the Password:** User receive an OTP for Login which is send to user valid mail id, figure 5.10 depict the password request as OTP.

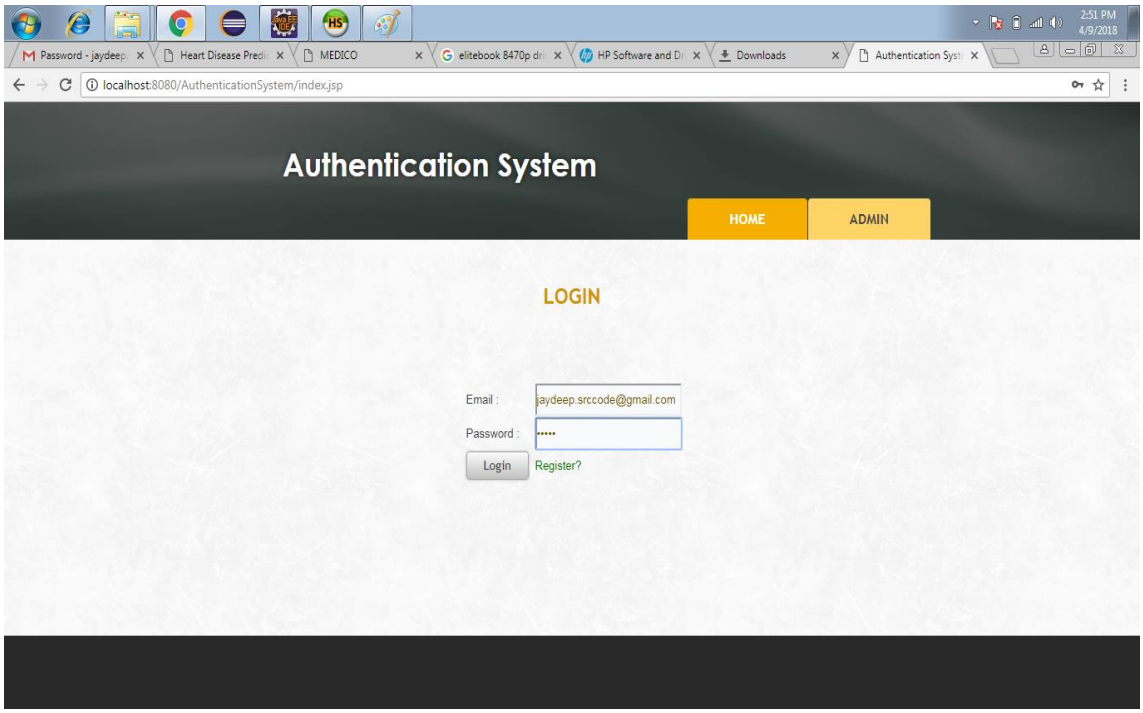

Figure 5.10: OTP as a Password

4. **Biometric Authentication:** Figure 5.11 and figure 5.12 shows the biometric authentication as third factor. Here we use face as a biometric characteristics.

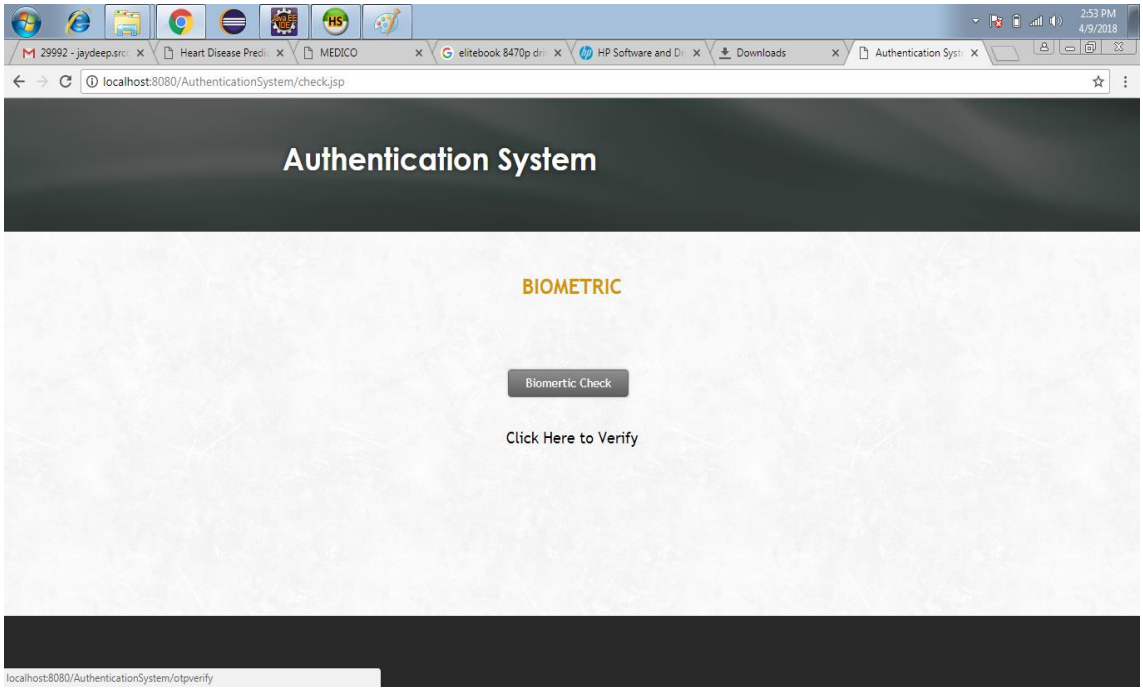

Figure 5.11: Biometric Authentication

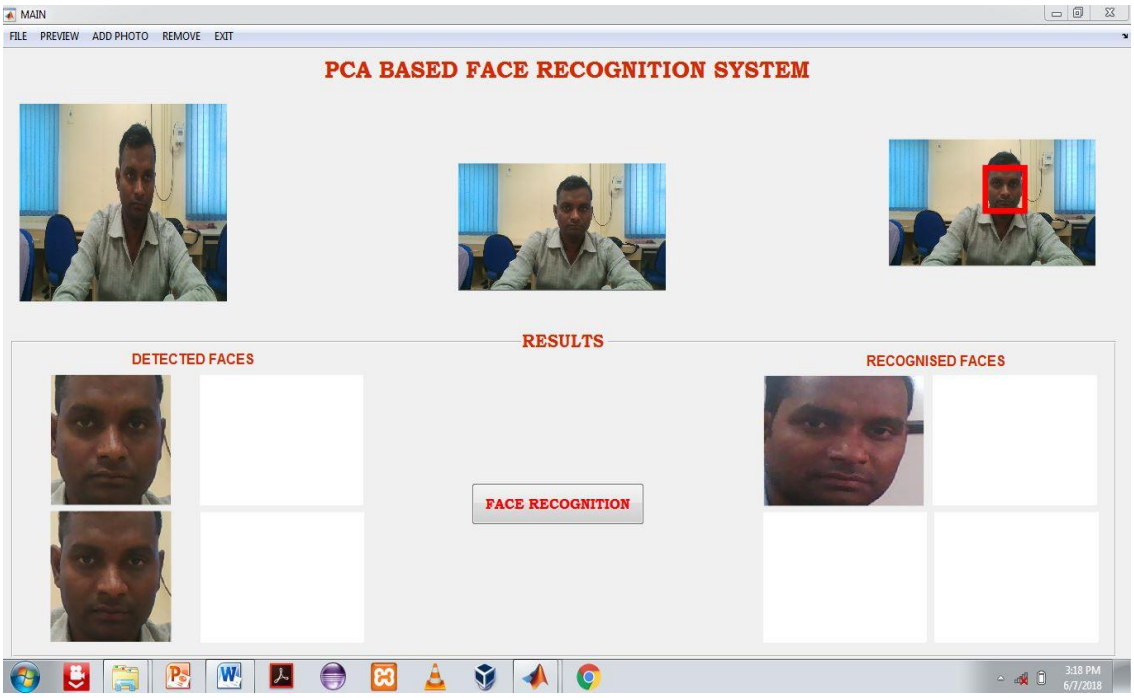

Figure 5.12: Face Capturing and Authentication

5. User Validation: user is verified by the system as authenticated user. Figure 5.13 depicts the confirmation page as valid user

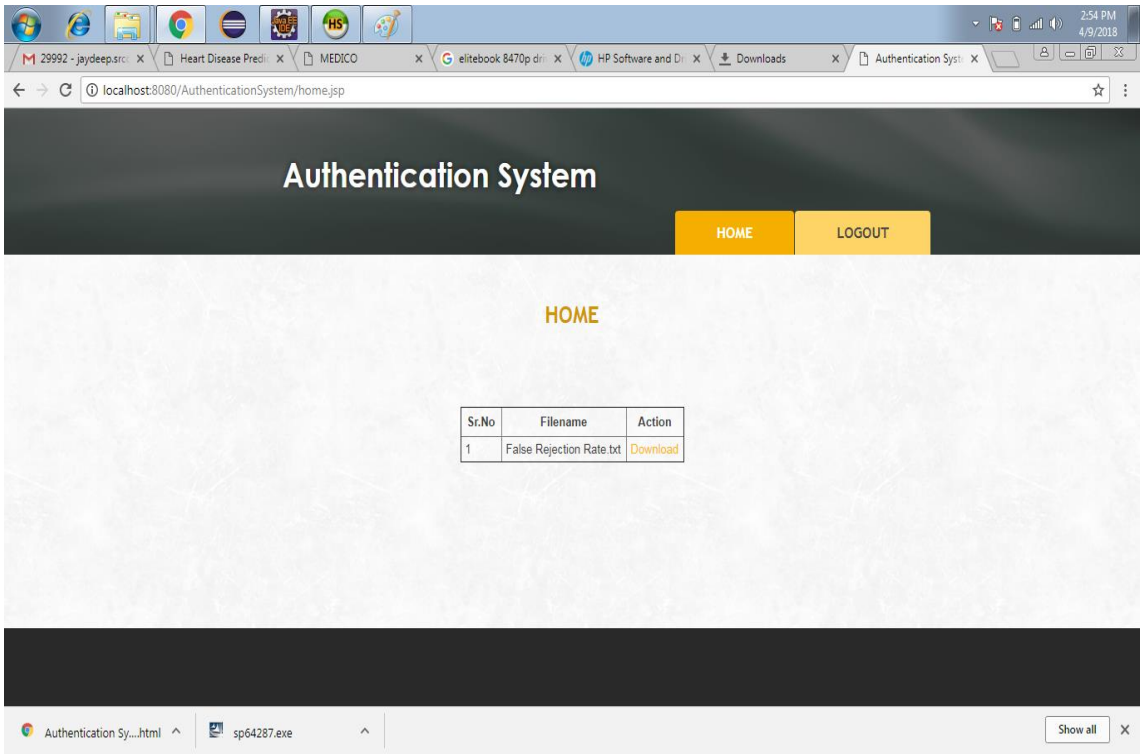

Figure 5.13: Verification/Authentication

6. **Send Request to Admin:** Figure 5.14 depicts the request to download the file.

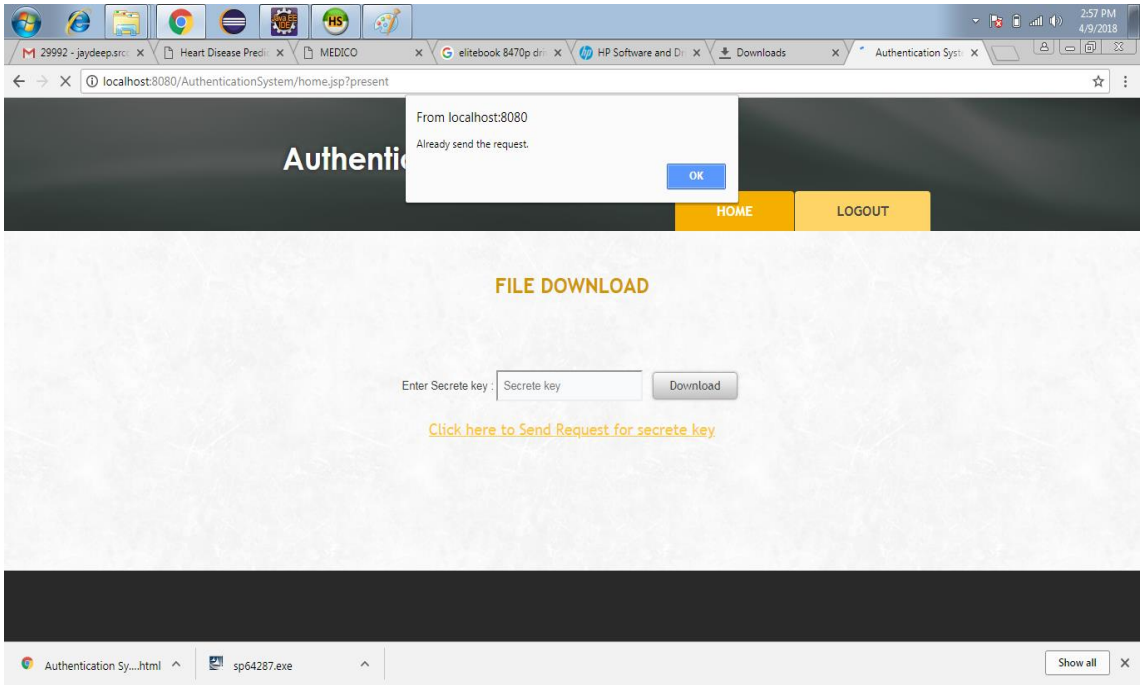

Figure 5.14: Service Access Request

7. **Validation of the Request**: In figure 5.14 the System admin validate the request and send a secret key to user valid email id after user validation.

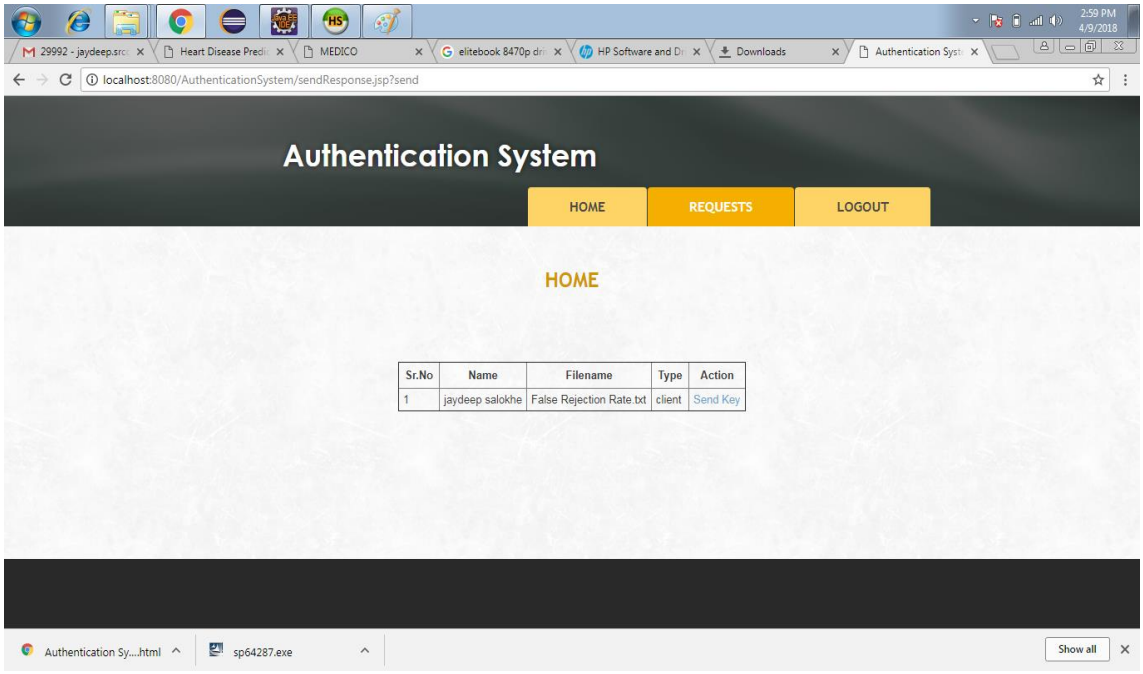

Figure 5.15: Validation of the Request

8. **Access Granted**: Now user enter secret key and download the file as shown in figure 5.16.

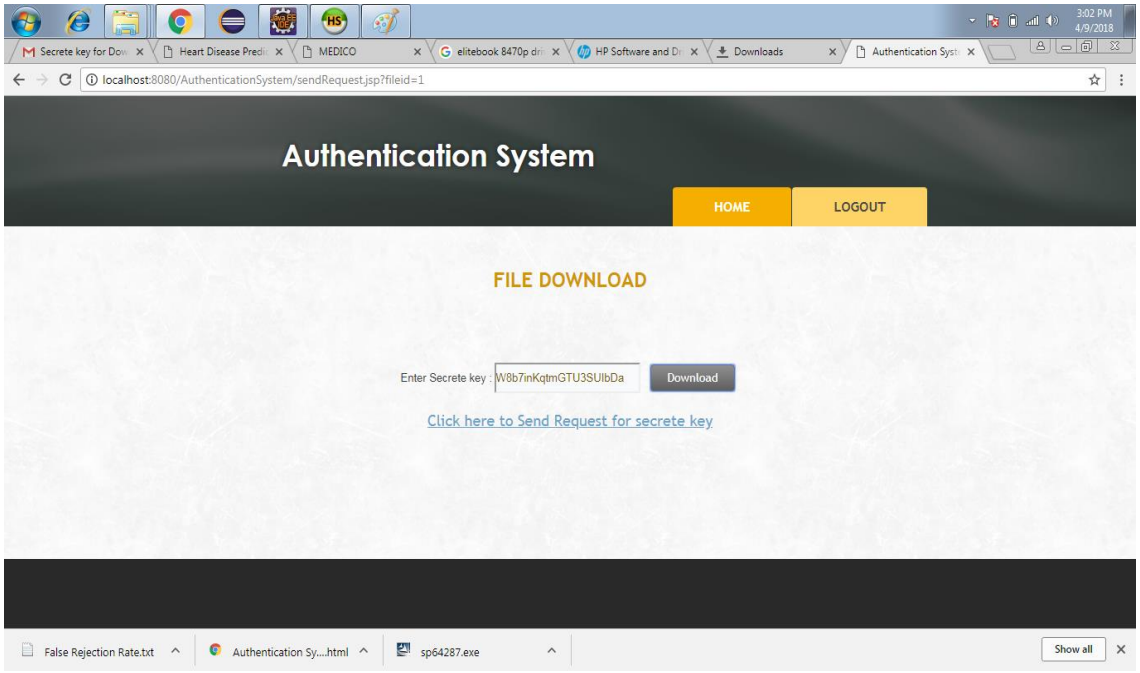

Figure 5.16: Access Granted

5.15. Conclusion

Multifactor authentication for access control has become the most important requirement for cloud computing to achieve the goals of secrecy, integrity and confidentiality. It is important to more closely integrate computer and network security to develop a true security discipline in the cloud. We use multi-factor access mechanisms to authenticate a person's identity. Therefore, increasing the number of authentication factors increases the complexity of access, but we have increased the security of user data. We believe that complexity is permissible with improved safety.