Chapter 1
INTRODUCTION

The objective is to upload a person's confidential details in one cloud and transfer it to another cloud after the user's unavailable. User details are stored in cloud and the user need to access his/her account at least once in every fifteen days. If the user fails to login, three times notification is sent to user through mail and mobile. If the user does not respond even after three notifications, the user consider as not available. Hence, the application transfers the user's data to account of user's nominee. By using this way, the user's confidential details are not destroyed after his unavailable. Rather, the nominee can access the user's personal data.

1.1 CLOUD: AMAZON SIMPLE STORAGE SERVICE (AMAZON S3)

Amazon Simple Storage Service (Amazon S3) is a scalable, high-speed, low-cost, web-based cloud storage service designed for online backup and archiving of data and application programs. S3 was designed with a minimal feature set and created to make web-scale computing easier for developers. Amazon S3 is object storage service, which differs from block and file cloud storage. Each object is stored as a file with its metadata included and given an ID number. Applications use this ID number to access an object. Unlike file and block cloud storage, a developer can access an object via a rest

API. The S3 cloud storage service gives a subscriber access to the same systems that Amazon uses to run its own websites. S3 enables a customer to upload, store and download practically any file or object that is up to five gigabytes (5 GB) in size. Amazon S3 comes in two storage classes: S3 Standard and S3 Infrequent Access. S3 Standard is suitable for frequently accessed data that needs to be delivered with low latency and high throughput. S3 Standard targets applications, dynamic websites, content distribution and big data workloads. S3 Infrequent Access offers a lower storage price for backups and long-term data storage.

WORKING WITH BUCKETS

Amazon does not impose a limit on the number of items that a subscriber can store; however, there are Amazon S3 bucket limitations. An Amazon S3 bucket exists within a particular region of the cloud. An AWS customer uses an Amazon S3 API to upload objects to a particular bucket. Customers configure and manage S3 buckets.

PROTECTING YOUR DATA

Subscriber data is stored on redundant servers in multiple data centers. S3 uses a simple web-based interface -- the Amazon S3 console -- and encryption for user authentication. A subscriber can choose to keep data private or make it publicly accessible. A user can also encrypt data prior to

storage. Rights may be specified for individual users. When a subscriber stores data on S3, Amazon tracks usage for billing purposes but does not otherwise access the data unless required to do so by law.

1.2 ELLIPTIC-CURVE CRYPTOGRAPHY (ECC)

Elliptic-curve cryptography is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security. Elliptic curves are applicable for key agreement, digital signatures, pseudo-random generators and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a symmetric encryption scheme. They are also used in several integer factorization algorithms based on elliptic curves that have applications in cryptography, such as Lenstra elliptic-curve factorization.

The small key sizes make ECC very appealing for devices with limited storage or processing power, which are becoming increasingly common in the IoT. In terms of more traditional web server use cases, the smaller key sizes can offer speedier SSL handshakes (which can translate to faster page load times) and stronger security.

ECC ENCRYPTION/DECRYPTION

Several approaches to encryption/decryption using elliptic curves have been analyzed in the literature. This one is an analog of the Megamall public-

key encryption algorithm. The sender must first encode any message m as a point on the elliptic curve Pm (there are relatively straightforward techniques for this). Note that the cipher text is a pair of points on the elliptic curve. The sender masks the message using random k, but also sends along a "clue" allowing the receiver who know the private-key to recover k and hence the message. For an attacker to recover the message, the attacker would have to compute k given G and kG, which is assumed hard.

Steps 1: first encode any message m as a point on the elliptic curve Pm

Steps 2: select suitable curve & point G as in D-H

Steps 3: A & B select private keys $nA<n$

Steps 4: compute public keys: $PA= nAG$, $PB= nBG$

Steps 5: A encrypts Pm : $Cm=\{kG, Pm + kPB\}$,

k: random positive integer

PB: B's public key

Steps 6: B decrypts Cm compute:

$$Pm + kPB – nB(kG) = Pm + k(nBG) – nB(kG) = Pm$$

Chapter 2

ABOUT THE PROJECT

2.1 PROBLEM DEFINITION:

- The aim of this work is to present the development of the application to be used in remember and deliver the secrets to nominee's account after the user unavailable.
- User details are stored in cloud and the user need to access his/her account at least once in every fifteen days. If the user fails to login, a notification is sent to user in every fifteen days through mail and mobile.
- If the user does not respond even after three notifications, the user consider as not available.
- Hence, the application transfers the user's data to account of user nominee. By using this way, the user's confidential details are not destroyed after his unavailable. Rather, the nominee can access the user's personal data.

2.2 ADVANTAGES

- Remembering things without any effort.
- It can keep things in storage.

2.3 EXISTING SYSTEM

- In existing system Reminders applications are used every day to help people to remember a task at an appropriate place or future time.
- Common methods for reminding are carefully placed post-it notes, email and electronic calendars.
- Unfortunately, these existing methods often lack the ability to trigger reminders at an appropriate place.

2.4 LIMITATIONS OF EXISTING SYSTEM

- Every existing system requires manual work of setting the reminder.
- Existing systems are time consuming because of manually setting the reminders.
- There is no facility to store the original documents in any of the existing system.
- There is no facility to remind about the confidential documents to the relatives.
- There is possibility of hanging down the existing systems due to the manual work.

2.5 PROPOSED SYSTEM:

The proposed system is an application to remind the personal information to the relatives through after the unavailable. This reminder will be set in the cloud with the help of the virtual brain application.

2.6 ADVANTAGES

- User relatives gets reminder on particular time.
- It also has a feature to select a range of dates in which he/ she should be alerted.
- To save documents, video, live video, audio and email accounts for creating reminders in future.
- To share current and saved information of the user by messaging or email services.

Chapter 3

SYSTEM REQUIREMENTS

The below requirements of both hardware and software are the minimum requirements.

3.1 HARDWARE REQUIREMENTS

Processor	: Dual core and above
Hard Disk	: 50 GB
RAM	: 1 GB

3.2 SOFTWARE REQUIREMENTS

Operating System	: Windows 8
Front End	: HTML with CSS, JavaScript
Scripting Language	: PHP
Back End	: MySQL

Chapter 4

TOOLS AND TECHNOLOGIES USED

4.1 HTML

HTML is the authoring language used to create documents on the web. It is used to define the structure and layout of a web page, how a page looks and any special functions.HTML mark-up consists of several key components, including those called tags (and their attributes), character-based data types, character references and entity references.

4.2 PHP

PHP is an "HTML-embedded scripting language" primarily used for dynamic Web applications. PHP takes most of its syntax from C, Java, and Perl. It is an open source technology and runs on most operating systems and with most Web servers. PHP originally stood for "Personal Home Page". The acronym was then formally changed to Hyper Text Pre-processor.

4.2.1 ADVANTAGES OF PHP

- Improved object-oriented programming
- Embedded SQLite
- Support for new MySQL features.
- Exception handling using a try..catch structure
- Integrated SOAP support
- The Filter library

4.3 JAVASCRIPT

JavaScript is a dynamic computer programming language. It is lightweight and most commonly used as a part of web pages, whose implementations allow client-side script to interact with the user and make dynamic pages. It is an interpreted programming language with object-oriented capabilities. JavaScript was first known as LiveScript, but Netscape changed its name to JavaScript, possibly because of the excitement being generated by Java. JavaScript made its first appearance in Netscape 2.0 in 1995 with the name LiveScript. The general-purpose core of the language has been embedded in Netscape, Internet Explorer, and other web browsers. The ECMA-262 Specification defined a standard version of the core JavaScript language.

- JavaScript is a lightweight, interpreted programming language.
- Designed for creating network-centric applications.
- Complementary to and integrated with Java.
- Complementary to and integrated with HTML.
- Open and cross-platform.

4.4 MySQL

The MySQL database server provides the ultimate in scalability, sporting the capacity to handle deeply embedded applications. A unique storage-engine architecture allows database professionals to configure the MySQL database

server specifically for particular applications, with the end result being amazing performance results. Rock-solid reliability and constant availability are hallmarks of MySQL, with customers relying on MySQL to guarantee around-the-clock uptime. MySQL offers a variety of high-availability options from high-speed master/slave replication configurations. By migrating current database-drive applications to MySQL, or using MySQL for new development projects, corporations are realizing cost savings that many times stretch into seven figures.

Chapter 5

SYSTEM DESIGN

5.1 CONTEXT ANALYSIS DIAGRAM

CAD LEVEL -0

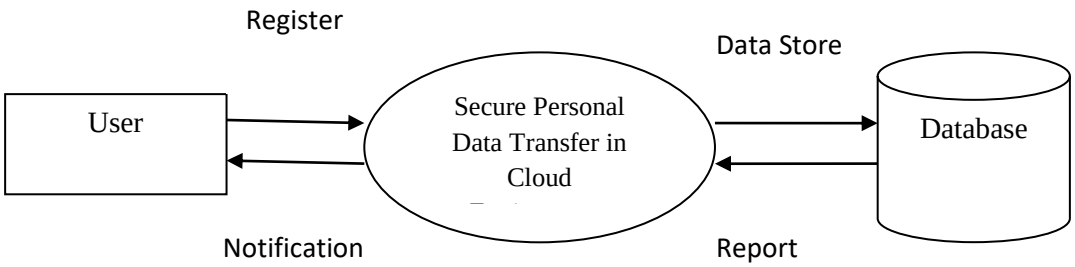

Fig 5.1 describes the context level analysis for the project.

LEVEL 1:

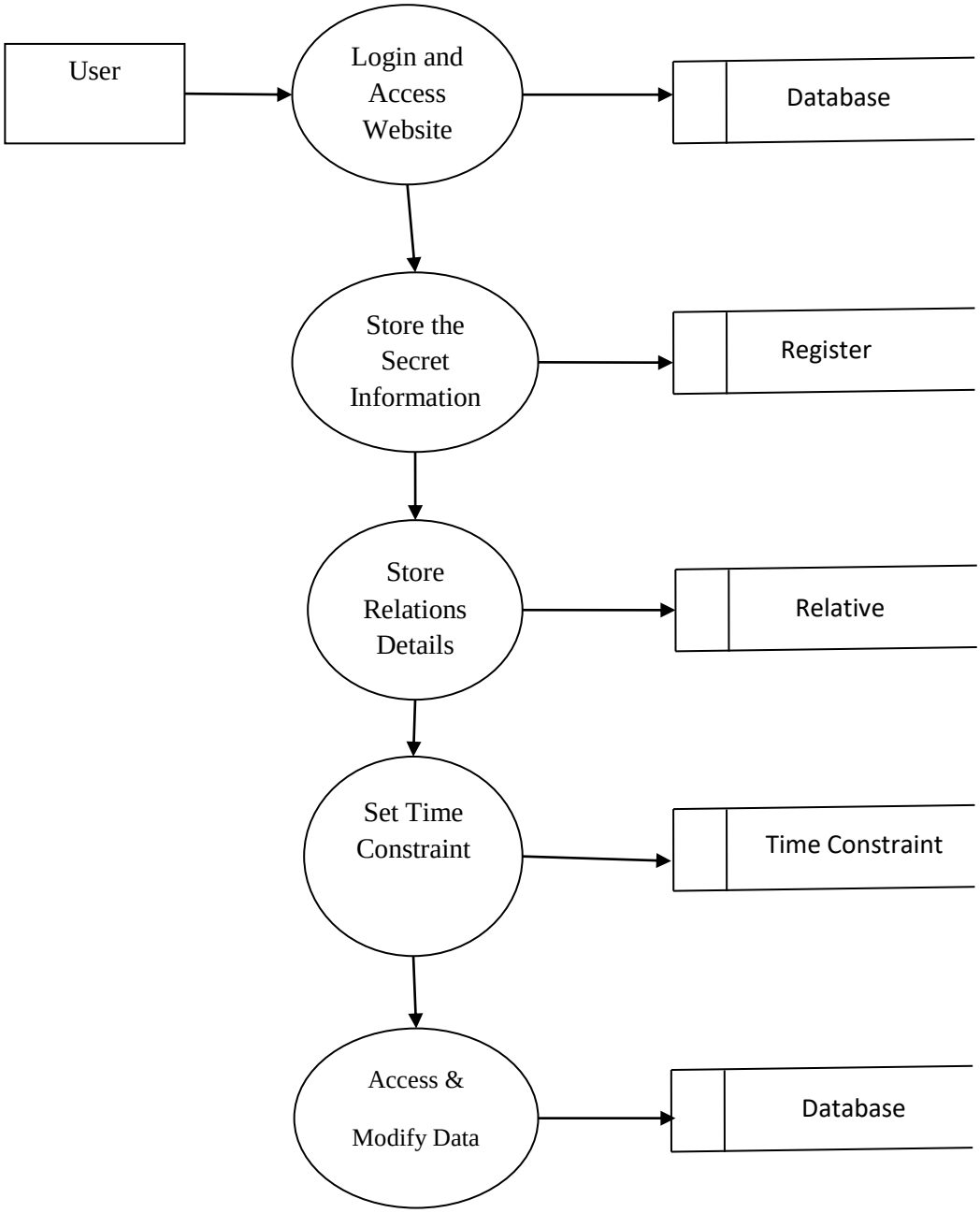

Fig 5.2 describes the data flow diagram for the project.

LEVEL 2:

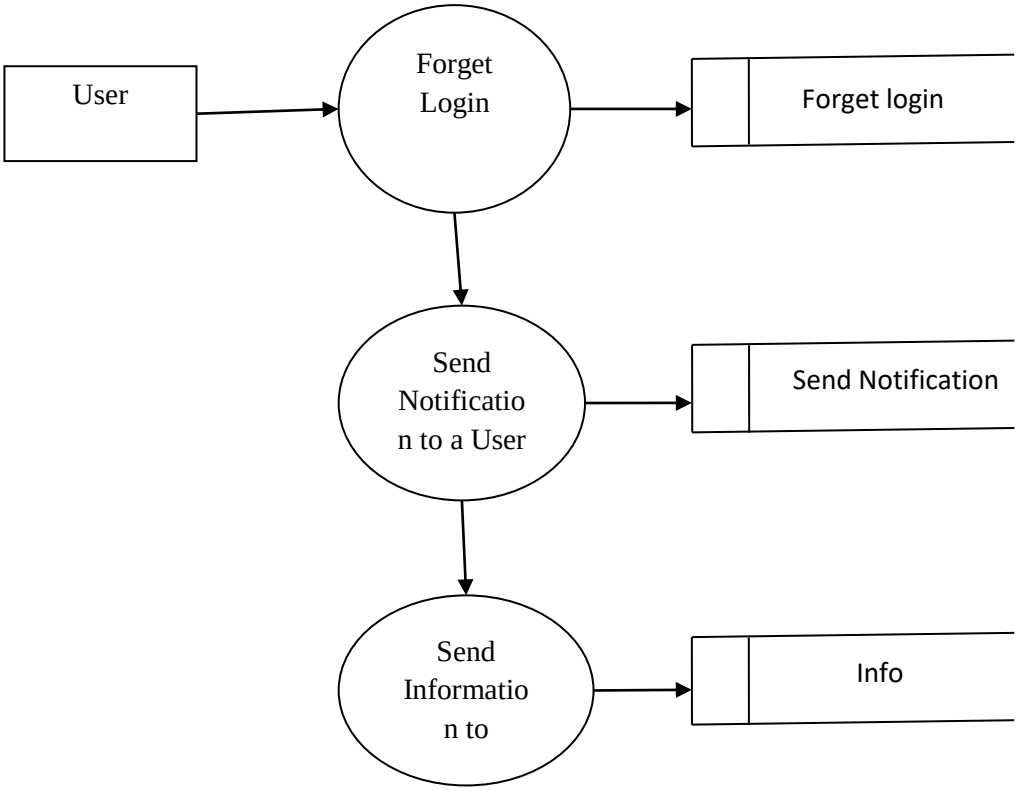

Fig 5.3 describes the data flow diagram for the project.

5.2 ER DIAGRAM

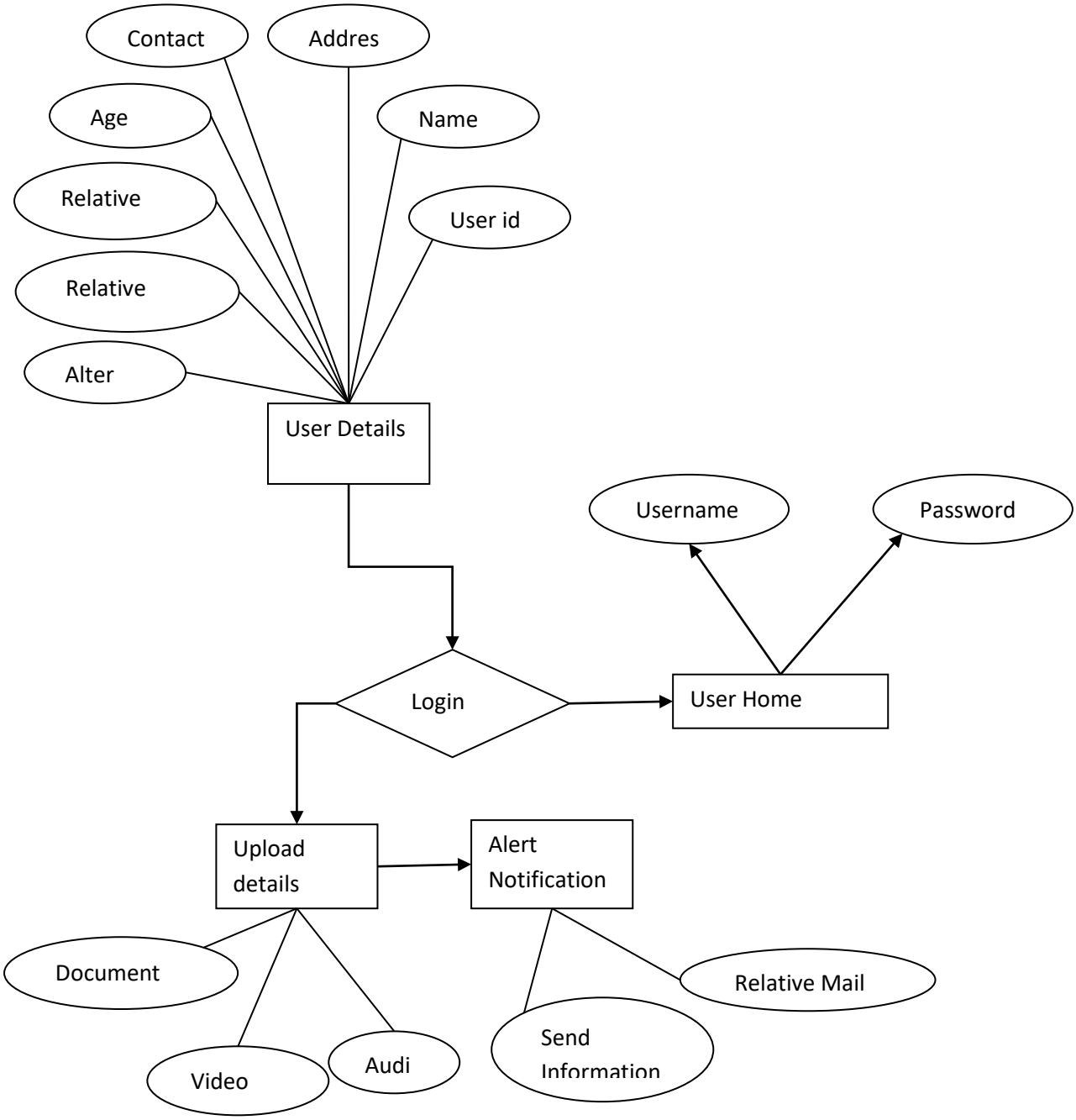

Fig 5.2.1 describes the entity relationship among the modules of the project.

5.3 DATABASE DESIGN

5.3.1 ACCOUNT TABLE

Field	Type	Null	Default
Id	int(11)	Yes	NULL
Rid	int(11)	Yes	NULL
Uname	varchar(30)	Yes	NULL
Bank	varchar(30)	Yes	NULL
branch	varchar(30)	Yes	NULL
account	varchar(30)	Yes	NULL
Pinno	varchar(10)	Yes	NULL
cardno	varchar(30)	Yes	NULL
acpass	varchar(30)	Yes	NULL
Rdate	varchar(15)	Yes	NULL

Table 5.3.1 describes the user account table design where the user details are stored in vb database.

5.3.2 AUDIO TABLE

Field	Type	Null	Default
Id	int(11)	Yes	NULL
Rid	int(11)	Yes	NULL
uname	varchar(30)	Yes	NULL
fileby	varchar(30)	Yes	NULL
ftype	varchar(20)	Yes	NULL

title	varchar(100)	Yes	NULL
details	varchar(200)	Yes	NULL
filename	varchar(100)	Yes	NULL

Table 5.3.2 describes the user audio table design where the user details are stored in vb database.

5.3.3 DOCUMENT TABLE

Field	Type	Null	Default
Id	int(11)	Yes	NULL
Rid	int(11)	Yes	NULL
uname	varchar(30)	Yes	NULL
Title	varchar(100)	Yes	NULL
details	varchar(200)	Yes	NULL
filename	varchar(100)	Yes	NULL
Rdate	varchar(15)	Yes	NULL

Table 5.3.3 describes the user document table design where the user details are stored in vb database.

5.3.4 EMAIL TABLE

Field	Type	Null	Default
Id	int(11)	Yes	NULL
Rid	int(11)	Yes	NULL
uname	varchar(30)	Yes	NULL
Email	varchar(40)	Yes	NULL

Pass	varchar(30)	Yes	NULL
Rdate	varchar(15)	Yes	NULL

Table 5.3.4 describes the user email table design where the user details are stored in vb database.

5.3.5 OCCUPATION TABLE

Field	Type	Null	Default
Id	int(11)	Yes	NULL
rid	int(11)	Yes	NULL
uname	varchar(30)	Yes	NULL
company	varchar(50)	Yes	NULL
position	varchar(50)	Yes	NULL
experience	varchar(100)	Yes	NULL
salary	varchar(30)	Yes	NULL
duration	varchar(50)	Yes	NULL
rdate	varchar(15)	Yes	NULL

Table 5.3.5 describes the user occupation table design where the user details are stored in vb database.

5.3.6 REGISTER TABLE

Field	Type	Null	Default
id	int(11)	Yes	NULL
fname	varchar(30)	Yes	NULL
lname	varchar(30)	Yes	NULL

gender	varchar(10)	Yes	NULL
dob	varchar(15)	Yes	NULL
address	varchar(50)	Yes	NULL
address2	varchar(50)	Yes	NULL
pincode	varchar(20)	Yes	NULL
city	varchar(30)	Yes	NULL
state	varchar(30)	Yes	NULL
country	varchar(30)	Yes	NULL
email	varchar(40)	Yes	NULL
mobile	bigint(20)	Yes	NULL
mobile2	bigint(20)	Yes	NULL
landline	varchar(20)	Yes	NULL
aadhar	varchar(20)	Yes	NULL
voter	varchar(20)	Yes	NULL
pancard	varchar(20)	Yes	NULL
driving	varchar(20)	Yes	NULL
sslc_school	varchar(50)	Yes	NULL
ug_per	Double	Yes	NULL
ug_year	varchar(20)	Yes	NULL
pg_college	varchar(50)	Yes	NULL
pg_per	Double	Yes	NULL
pg_year	varchar(20)	Yes	NULL

photo	varchar(50)	Yes	NULL
uname	varchar(30)	Yes	NULL
pass	varchar(30)	Yes	NULL
last_date	varchar(15)	Yes	NULL
secret	varchar(20)	Yes	NULL
sms_st	int(11)	Yes	NULL
status	int(11)	Yes	NULL
rid	int(11)	Yes	NULL
rdate	varchar(15)	Yes	NULL

Table 5.3.6 describes the user register table design where the user details are stored in vb database.

5.3.7 RELATIVE TABLE

Field	Type	Null	Default
id	int(11)	Yes	NULL
uname	varchar(30)	Yes	NULL
name	varchar(30)	Yes	NULL
relation	varchar(30)	Yes	NULL
mobile	bigint(20)	Yes	NULL
email	varchar(40)	Yes	NULL
pass	varchar(20)	Yes	NULL
rdate	varchar(15)	Yes	NULL

Table 5.3.7 describes the user relative table design where the user details are stored in vb database.

Chapter 6

SYSTEM IMPLEMENTATION

Implementation includes all those activities that take place to convert from the old system to the new. The old system consists of manual operations, which is operated in a very different manner from the proposed new system. A proper implementation is essential to provide a reliable system to meet the requirements of the organization. The implementation is a process of converting the design into source code. The project developed by using front end as HTML, CSS and back end as PHP and MySQL Database. The following mysql functions are used in this project for database related activities.

- **MYSQL_CONNECT ()** query are used to make a connection to the SQL database.
- **MYSQL_SELECT_DB ()** query are used to select a database.
- **MYSQL_QUERY()**query are used to create or delete a MySQL database
- **MYSQL_CLOSE ()** query are used to close the database connection.
- **MYSQL_FETCH_ARRAY ()** can be used to fetch all the selected data. This function returns row as an associative array, a numeric array, or both.
- **MYSQL_FETCH_ASSOC ()** which return the row as an associative array.
- **AVG** function is used to find out the average of a field in various records.
- In addition to this, **INPUT** and **SELECT** tags are used for getting the input from the user. The FORM tags are used to transfer the data to the server.

Chapter 7

SYSTEM TESTING

7.1 TES TING OBJECTIVE

- Testing is the process of executing a program with the intent of finding errors.
- A good test is one that has probability of finding an undiscovered error.
- A successful test is one that uncovers a yet undiscovered error.

7.2 TESTING STRATEGIES

- To verify all the images on the web page are displayed properly on all the different devices and resolution.
- To verify text and headings on the web page are properly aligned.
- To verify all the clickable links on the web page are readable and work as expected.
- To verify scrolling of the web page works as expected.
- To verify if there are input boxes and text areas to enter data then we need to make sure that the text entered is displayed properly on the web page and they are aligned as expected.
- To verify image size, Font size and font type are consistent across all the web pages.
- To verify if contents of the page are displayed consistent on all resolutions.

- To verify the color changes after hover over the elements.
- To verify the consistency of color combination on different resolutions.
- To verify images, text, different controls are not going beyond the screen border.

Chapter 8

CONCLUSION

This Project title is Building a Secure Personal Data Transfer in Cloud Environment to life for the secrets. This project was developed to store the secret information of the user. User can store their secret information into this site. Then login and view the information and also modify the information. When the user is not available the information was shared to user's relatives or friends. This system was implemented successfully. Then information was secured using this website. With the advancements in technology, user who is the ultimate source of information and discovery should also be preserved. A user does not live for thousands of years but the information in their mind could be saved and used for several thousands of years. The whole idea is that memory, mental illness and perception triggered by neurons and electric signals could be soon treated with a supercomputer that models nearly all the 1,000,000 million synapses of the brain.

Chapter 9

BIBLIOGRAPHY

REFERENCES:

- https://blog.cloudsecurityalliance.org/2011/09/30/securing-your-file-transfer-in-the-cloud/secure data transfer in cloud computing
- https://www.researchgate.net/profile/Dr_K_Wagh/publication/264229298_Securing_Data_Transfer_in_Cloud_Environment/links/553ca2a00cf29b5ee4b89e69/Securing-Data-Transfer-in-Cloud Environment.pdf