Security Approach for Multi-Cloud Data Storage

Mandar Kadam
St. Francis Institute of Technology, Borivali (west), Mumbai, India

Stewyn Chaudhary
St. Francis Institute of Technology, Borivali (west), Mumbai, India

Bony Carvalho
St. Francis Institute of Technology, Borivali (west), Mumbai, India

ABSTRACT

In many organizations, transformation of information and storage of sensitive data has highest priority. Client data should be kept secret as well as inaccessible from all other unauthorized hacks [1]. To maintain the security of the user data, cloud computing environment has practiced. The cloud computing is a cost-effective, service availability, flexible and on demand service delivery platform for providing business through the internet [2].

However, as the security of a single cloud is concerned, it fails to provide a strong protection layer against the malicious attacks. So, there is always a risk of data unavailability in system failure. A movement towards of “multi clouds” or “multiple clouds‟ or “cloud-of-clouds” has emerged currently using Shamir’s Secret Sharing Algorithm [3]. Here, the implementation of Shamir’s secret sharing algorithm is performed to authenticate a unique user and to access a particular file from the cloud storage.

General Terms

Security, Cloud Computing.

Keywords

Shamir’s Secret Sharing Algorithm, Data Security, Cloud Storage, Single Cloud, Multi Clouds Authentication.

1. INTRODUCTION

Now days, many organizations are relied on sharing of information. This information contains user private data as well as high secure data. Therefore need for secure and robust data resources are increased rapidly. Cloud data storage is a major solution to overcome this problem. Using a cloud storage services enables the users to access their information from any point in the world. But data stored on a ‘Single cloud’ may lead the highest risk to loss the data permanently if an interruption to its operation is invoked. The dealing with ‘single cloud’ providers is becoming less satisfactory service with customers because of major problems such as service availability failure for some time and malicious insider’s attacks in the single cloud [2]. Hence, to provide a secure way to access a data need move towards ‘Multiple clouds’ or ‘Cloud of Clouds’.

In proposed system, cluster of cloud storage is created and maintained accordingly to satisfy the user specific data access requirements. Here the replication of the user data to multiple clouds is done and update that information timely. Therefore loss of data from single cloud does not create a permanent loss of information. The data access mechanism is implemented using Shamir’s Secret Sharing algorithm which generates the secret keys to authenticate the user. As the priority is given to the user data, it is also important to make available this data to a right person. Therefore, the secret keys are shared to the user via his or her mail id which is taken while registering a new user. It plays a role of double authentication to identify the unique person. Here, to access a file from cloud storage, user must provide the same set of secret keys with any threshold value. Also to provide more security to user data, Advanced Encryption Standard (AES) algorithm is used to encrypt the user data.

2. LITERATURE SURVEY

2.1 HAIL Model

Mohammed A. Alzain, Ben Soh and Eric Pardete [4] describes, it is a distributed cryptographic system (High Availability and Integrity Layer) that allows a set of servers to prove to a client that a stored file is intact and retrievable. HAIL relies on a single trusted verifier. It aggregates cryptographic protocols for proof of recoveries with erasure codes to provide a software layer to protect the integrity and availability of the stored data, even if the individual clouds are compromised by a malicious and mobile adversary. HAIL has at least three limitations: it only deals with static data, it requires that the servers run some code and does not provide guarantee of confidentiality of the stored data.

2.2 DepSky Model

Alysson Bessani, Miguel Correia, Bruno Quaresma, Fernando Andre, Paulo Sousa [5] describes, the increasing popularity of cloud storage services has lead companies that handle critical data to think about using these services for their storage needs. However, the reliability and security of data stored in the cloud still remain major concerns. In this work, DepSky model is studied, a system that improves the availability, integrity, and confidentiality of information stored in the cloud through the encryption, encoding, and replication of the data on diverse clouds that form a cloud-of-clouds. Moreover, the monetary costs of using DepSky in this scenario is at most twice the cost of using a single cloud, which is optimal and seems to be a reasonable cost, given the benefits.

2.3 Survey on need for multi-clouds:

S.Subashini, V.Kavitha [6] says, Cloud computing usage has increased rapidly in many companies. Cloud computing offers many benefits in terms of low cost and accessibility of data. Ensuring the security of cloud computing plays a major role in the cloud computing, as customers often store important information with cloud storage providers but these providers may be unsafe. Dealing with “single cloud” providers is predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud. A movement towards “multi-clouds”, or in other words, “inter-clouds” or “cloud-of-clouds" has increased recently. The purpose of authors is to survey recent research related to single and multi-clouds security and to address possible solutions. It is found that the research into the use of multi-cloud providers to maintain security has received less attention from the research community than has the use of single clouds. Their work aspires to promote the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing consumer.

3. PROPOSED WORK

Our proposed system contains the cluster of cloud storages. It may call as "Cloud of clouds" or "multi clouds". These individual clouds are interconnected to each other. Here ,the user uploaded file is replicated on more than one cloud storage, that is two to three different interconnected but individual clouds. User host machine implements Shamir's secret sharing algorithm and it is responsible to generate the set of secret keys. To access a particular file, user must input a set of secret keys with minimum threshold vlaue. Therefore, using these secret keys, machine can easily authenticate the user.

Fig. 1 describes the flow of the user activities. To start the interaction with the system, first user must register to the system. After login, user always has two options, to upload a file on cloud or to download a file from cloud. To upload a file on cloud, user simply selects a file to be uploaded and put it on the cloud.

Our system assigns a unique number to the file which is used by Shamir's Secret Sharing algorithm to generate the set of secret keys. As shown in a figure 2, this file is encrypted using 256 bit Advanced Encryption Standard (AES) algorithm. And afterwards, this file will replicate on multi-clouds. Here, three different cloud storages are taken into consideration.

On the other hand, while downloading the file, as shown in a figure 3, user must specify the file name as well as from which cloud storage user has to download it. This functionality adds flexibility to the process as user has choice to select best cloud storage provider's service. After this, Shamir's Secret Sharing algorithm is implemented to generate the secret keys. In our proposed solution, secret keys are shared with the user through his or her mail id. It has shown in figure 4 that ten secret keys are send to the client's mail id. This way of sharing enhances the data security layer with double authentication process. If the secret keys are match with threshold value then the user is allowed to download the file. However, first the file is decrypted and then it is being downloaded. Figure 5, shows the interface to insert the secret keys with threshold of 6 secret keys. To download a file, user must give the input of same secret keys as that in the mail id.

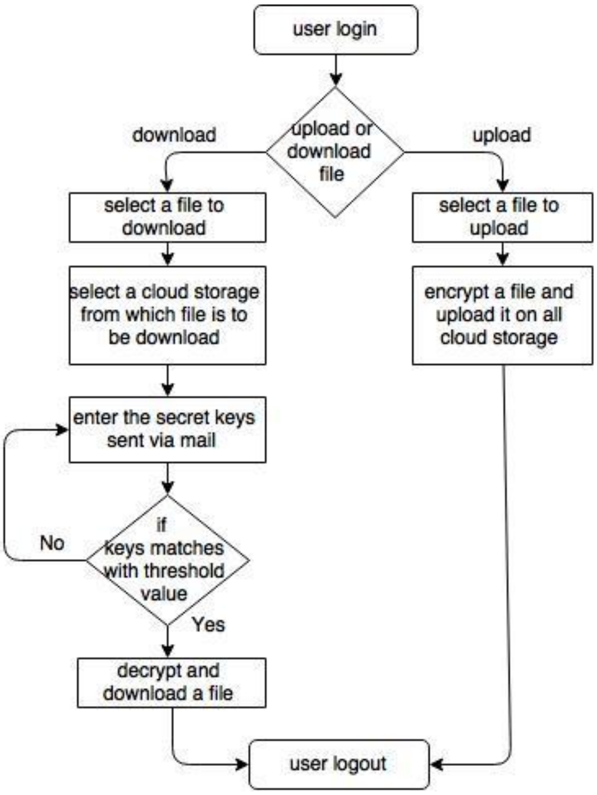

user login
upload or download file
download
upload
select a file to download
select a file to upload
select a cloud storage from which file is to be download
encrypt a file and upload it on all cloud storage
enter the secret keys sent via mail
No
if keys matches with threshold value
Yes
decrypt and download a file
user logout

Figure 1: User level working flow

Figure 1 illustrates how the user will interact to the system.

To manage the users' activity, the system administrator is introduced. System administrator has rights to authenticate the user and to update the user information.

3.1 Shamir's secret sharing algorithm

3.1.1 Preparation

Suppose that our secret is 1234 $(S = 1234)$.

In this proposed solution, consider 'S' is the file name (which is unique number assigned) stored in the database after uploading that file on cloud.

Divide the secret into 6 parts $(n = 6)$, where any subset of 3 parts $(k = 3)$ is sufficient to reconstruct the secret. At random one can obtain two ($k - 1$) numbers: 166 and 94.

$$(a_1 = 166; a_2 = 94)$$

Our polynomial to produce secret shares (points) is therefore:

$$f\ (x)\ = 1234 + 166x + 94x^2$$

Construct 6 points $D_{x-1} = (x, f(x))$ from the polynomial:

$$D_0 = (1,1494); D_1 = (2,1942); D_2 = (3,2578); D_3 = (4,3402); D_4 = (5,4414); D_5 = (6,5614)$$

Give each participant a different single point (both x and $f\ (x)$). Because here, use D_{x-1} instead of D_x the points start from $(1\,,f(1))$ and not $(0,f(0))$. This is necessary because if one would have $(0,f(0))$ he would also know the secret ($S\ =\ f(0)$)

Here, D_0 , D_1, D_2, D_3, D_4, D_5 are corresponding set of secret keys for file name 'S'.

3.1.2 *Reconstruction*

In order to reconstruct the file name 'S' any 3 points will be enough.

Let us consider

$$(x_0, y_0) = (2,1942); (x_1, y_1) = (4,3402); (x_2, y_2) = (5,4414)$$

Now, compute Lagrange basis polynomials:

$$\ell_0 = \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} = \frac{x-4}{2-4} \cdot \frac{x-5}{2-5} = \frac{1}{6}x^2 - \frac{3}{2}x + \frac{10}{3}$$

$$\ell_1 = \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2} = \frac{x-2}{4-2} \cdot \frac{x-5}{4-5} = -\frac{1}{2}x^2 + \frac{7}{2}x - 5$$

$$\ell_2 = \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1} = \frac{x-2}{5-2} \cdot \frac{x-4}{5-4} = \frac{1}{3}x^2 - 2x + \frac{8}{3}$$

Therefore

$$f(x) = \sum_{j=0}^{2} y_j \cdot \ell_j(x)$$

$$= 1234 + 166x + 94x^2$$

Recall that the secret is the free coefficient, which means that $S\ =\ 1234$ [7]

Therefore, the file name is reconstructed.

4. IMPLIMENTATION

Implemented of this proposed solution is performed by making a web application. Enhanced the front end with Cascading Style Sheet (CSS) web programming language and server side scripting is done in ASP.net. Three different databases are created as analogy to cloud storage. And these database scripting is done with C# and connected with local host. File uploaded on a single database will be replicated to other two databases.

One host machine is also developed, which implements Shamir's Secret Sharing Algorithm and generates the secret key and sends it to the user as well. This machine also implements 256 bit Advanced Encryption Standard (AES) algorithm.

5. RESULTS

Table 1 Result Analysis

Test Case	Expected Result	Actual Result
Registration with correct user details	User should be allowed to create new account	User was able to create new account
Registration with incorrect user details	User should not allowed to create new account and must display "incorrect details"	User was unable to create new account and message displayed as "incorrect details"
Login with correct username and password	User should be successfully login to account	User was able to login successfully
Login with incorrect username and password	User should not be allowed to login and must display "incorrect username and password"	Website application displayed "incorrect username and password"
Uploading file with valid file format	User should be allowed to upload file on cloud storage	Application allowed user to upload file on cloud storage
Uploading file with invalid file format	User should not be allowed to upload file on cloud storage	User not allowed to upload a file on cloud storage
Inserting correct secret keys	Application should allow user to download the required file	Access was given by the application to download the required file
Inserting wrong secret keys	Application should not allow user to download the required file	Access was denied by application to download the file
Sending auto mail consisting secret keys	Mail must be send to corresponding registered user	Mail has sent to the registered user

6. CONCLUSION AND FUTURE SCOPE

There are some combined benefits of multi-clouds and secret sharing scheme, such as, infrastructure deployment, data accessibility, user authentication etc. Multi-cloud is looking to be more secure, harder to compromise over single cloud data storage. Cloud computing is currently the latest trend when it comes to online computing, it may help the enterprise and the end user by providing their needs, but the provider has to make sure that they are valuable and customer data is safe[8].

In future scope, the applications of this project are numerous. This application can be used by schools and colleges to share important data with a specific faculty. This can also be used by Universities to share confidential data with the listed colleges, for example, sharing examination question paper with the principal of colleges. In different business firms, this concept cloud is used to share confidential details with their clients.

7. ACKNOWLEDGMENTS

We wish to offer our sincere thanks to each and every person who has helped us either directly or indirectly during the course of this paper.

Above all we wish to thank our Project Guide, Mr. Rajkumar Shende for his valuable assistance and advice. Special thanks to the faculty member of the Computer Engineering Department of St. Francis Institute of Technology for their approval and guidance.

We also wish to express our deepest gratitude to our fellow students and friends who have contributed in some way to our project.

8. REFERENCES

[1] Mohammed A. AlZain, Ben Soh, Eric Pardede, “A Survey on Data Security Issues in Cloud Computing: From Single to Multi-Clouds”, Journal of Software, Vol 8, No 5 (2013), 1068-1078, May 2013

[2] Hassan Takabi, James B.D., Joshi, Gail-Joon, Ahn, “Security and Privacy Challenges in Cloud Computing Environments”, University of Pittsberg, October 2010.

[3] Md Kausar Alam, Sharmila Banu K, “An Approach Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds”, International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013

[4] Mohammed A. AlZain, Ben Soh and Eric Pardede, “Cloud computing security: from single to multi-clouds”, 2012, 45th Hawaii international conference on system sciences.

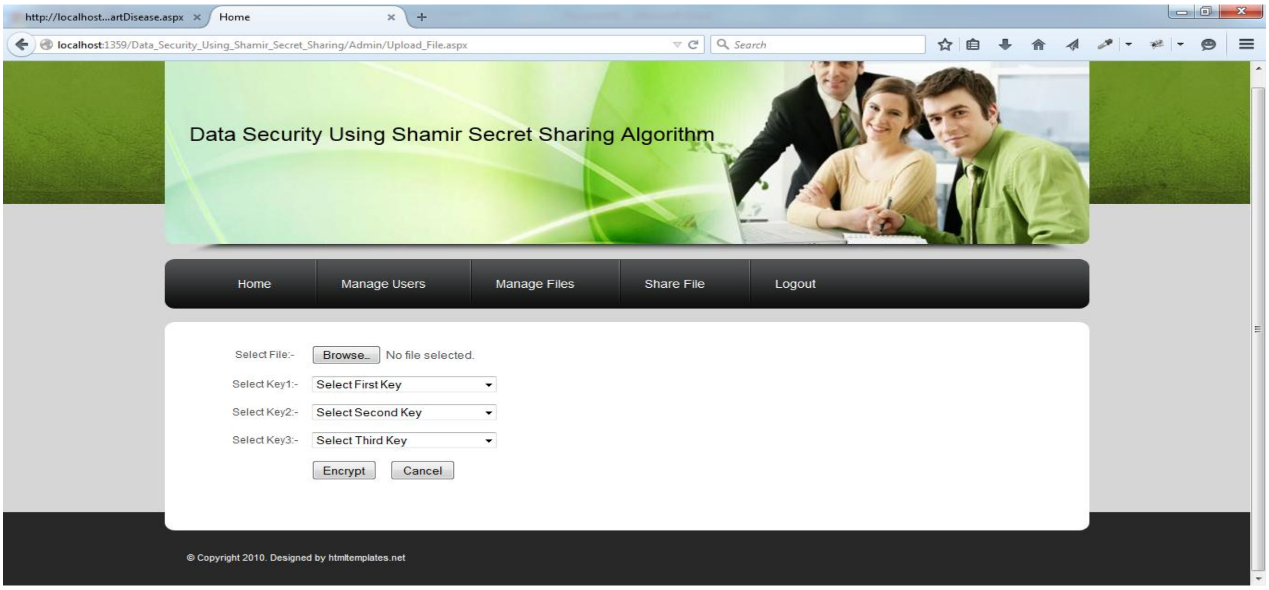
[5] Alysson Bessani, Miguel Correia, Bruno Quaresma, Fernando Andre, Paulo Sousa, “DEPSKY: Dependable and Secure Storage in a Cloud-of-Clouds”, University of Lisbon, Faculty of Sciences, Portugal.

[6] S. Subashini, V.Kavitha, “A surveys on security and privacy issues in service delivery models of the cloud computing”, journal of networks and computer applications, 34 (1), 2011, pp1-11.

[7] Shamir, Adi (1979), "How to share a secret", Communications of the ACM 22 (11): 612–613

[8] Review of methods for secret sharing in cloud Computing- “International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)”, Volume 2, Issue 1, January 2013

9. APPENDIX


http://localhost...artDisease.aspx
Home
localhost:1359/Data_Security_Using_Shamir_Secret_Sharing/Admin/Upload_File.aspx
Search
Data Security Using Shamir Secret Sharing Algorithm
Home
Manage Users
Manage Files
Share File
Logout
Browse...
Encrypt
Cancel

Select File:- No file selected.

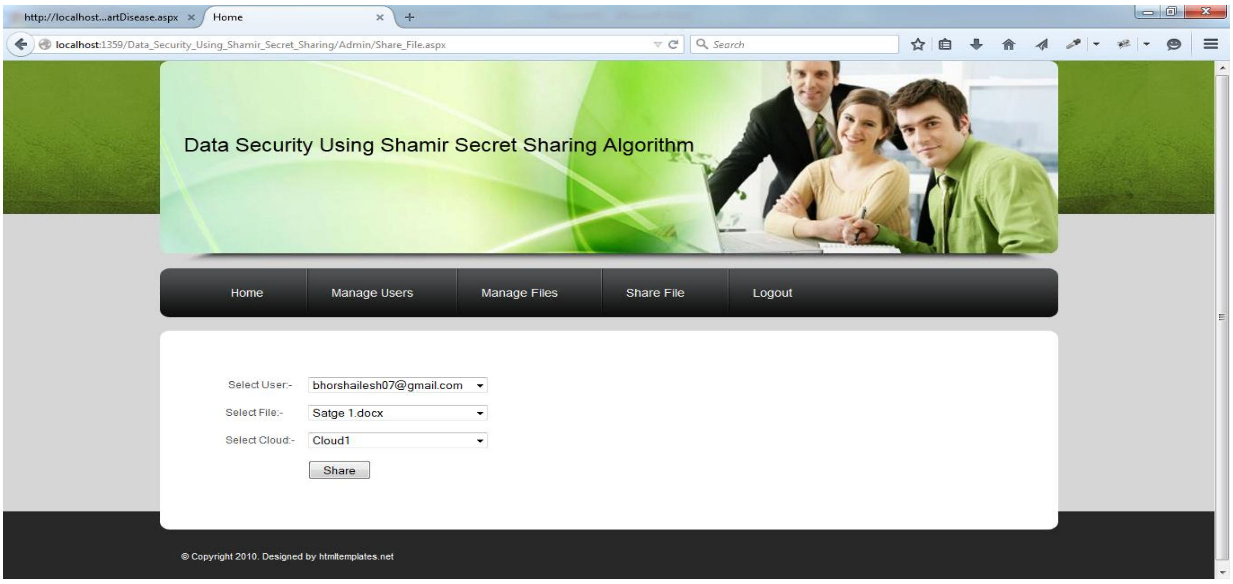
Select Key1:- Select First Key

Select Key2:- Select Second Key

Select Key3:- Select Third Key

© Copyright 2010. Designed by htmltemplates.net

Figure 2: Webpage for file encryption and file upload

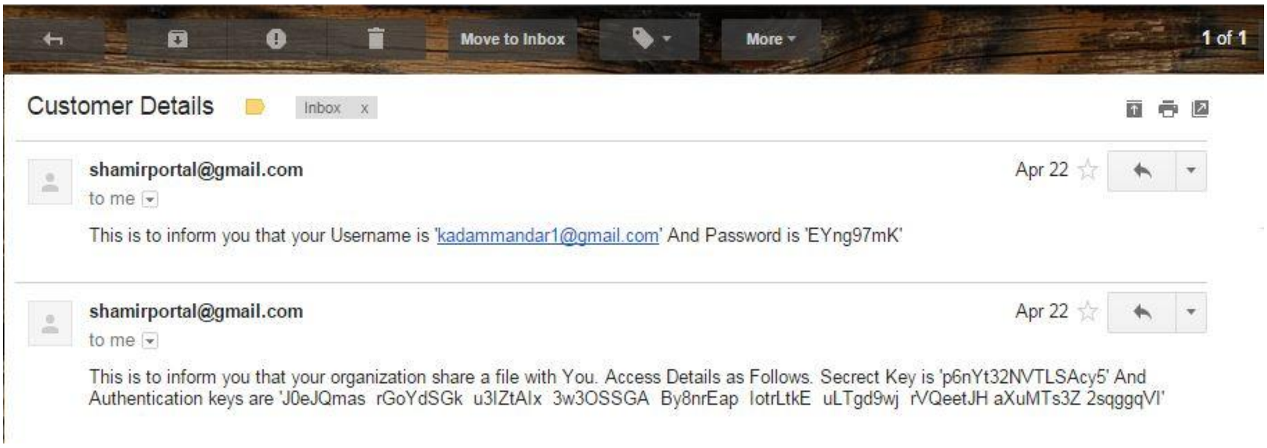

http://localhost...artDisease.aspx
Home
localhost:1359/Data_Security_Using_Shamir_Secret_Sharing/Admin/Share_File.aspx
Search
Data Security Using Shamir Secret Sharing Algorithm
Home
Manage Users
Manage Files
Share File
Logout
Share
© Copyright 2010. Designed by htmltemplates.net

Select User:- bhorshailesh07@gmail.com

Select File:- Satge 1.docx

Select Cloud:- Cloud1

Figure 3: Webpage for sharing a file to download it



Customer Details

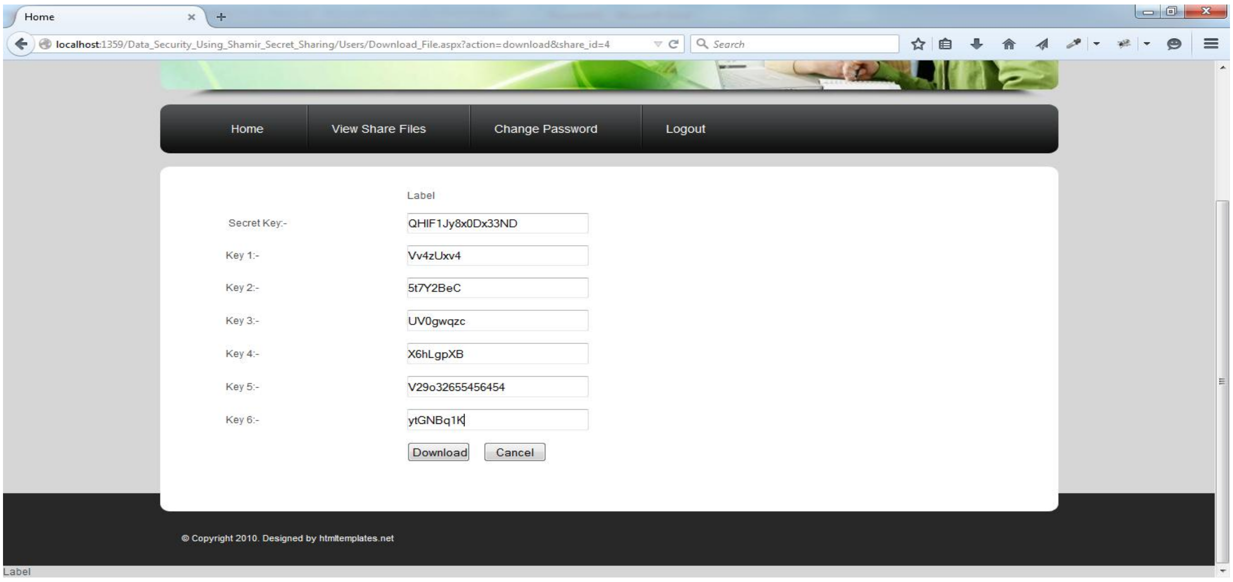
shamirportal@gmail.com
to me
Apr 22

This is to inform you that your Username is 'kadammandar1@gmail.com' And Password is 'EYng97mK'

shamirportal@gmail.com
to me
Apr 22

This is to inform you that your organization share a file with You. Access Details as Follows. Secrect Key is 'p6nYt32NVTLSAcy5' And Authentication keys are 'J0eJQmas rGoYdSGk u3lZtAlx 3w3OSSGA By8nrEap lotrLtkE uLTgd9wj rVQeetJH aXuMTs3Z 2sqggqVl'

Figure 4: Secret keys are mailed to the client


Home
localhost:1359/Data_Security_Using_Shamir_Secret_Sharing/Users/Download_File.aspx?action=download&share_id=4
Search
Home
View Share Files
Change Password
Logout
Label
Download
Cancel
© Copyright 2010. Designed by htmltemplates.net
Label

Secret Key:- QHIF1Jy8x0Dx33ND

Key 1:- Vv4zUxv4

Key 2:- 5t7Y2BeC

Key 3:- UV0gwqzc

Key 4:- X6hLgpXB

Key 5:- V29o32655456454

Key 6:- ytGNBq1K

Figure 5: Webpage for inserting the secret keys