

## **STRONG KEY-EXPOSURE RESILIENT AUDITING FOR SECURE CLOUD STORAGE**

A. Durga Devi<sup>1</sup>, K. Jahnavi,

<sup>1</sup>Assistant professor(HOD) , PG DEPT, Dantuluri Narayana Raju College, **Bhimavaram, Andharapradesh**  
**Email:-adurgadevi760@gmail.com**

<sup>2</sup>PG Student of PG, Dantuluri Narayana Raju College, **Bhimavaram, Andharapradesh**  
**Email:- anuhya092001@gmail.com**

### **ABSTRACT**

Key exposure is one serious security problem for cloud storage auditing. In order to deal with this problem, cloud storage auditing scheme with key-exposure resilience has been proposed. However, in such a scheme, the malicious cloud might still forge valid authenticators later than the key-exposure time period if it obtains the current secret key of data owner.

In this paper, we innovatively propose a paradigm named strong key exposure resilient auditing for secure cloud storage, in which the security of cloud storage auditing not only earlier than but also later than the key exposure can be preserved. We formalize the definition and the security model of this new kind of cloud storage auditing and design a concrete scheme. In our proposed scheme, the key exposure in one time period doesn't affect the security of cloud storage auditing in other time periods. The rigorous security proof and the experimental results demonstrate that our proposed scheme achieves desirable security and efficiency.

### **1 INTRODUCTION**

Nowadays, cloud storage is becoming one of the most attractive choices for individuals and enterprises to store their large scale of data. It can avoid committing large capital of users for purchasing and managing hardware and software. Although the benefits of cloud storage are tremendous, security concerns become significant

challenges for cloud storage. One major concern on cloud storage security is about the integrity of the data stored in cloud. Because clients lose the control of their data stored in cloud and data loss might happen in cloud storage, it is natural for clients to doubt whether their data are correctly stored in cloud or not.

Cloud storage auditing, as one effective security technique, is proposed to ensure the integrity of the data stored in cloud. Many cloud storage auditing schemes have been proposed up to now [1–13]. These schemes consider several different aspects of cloud storage auditing such as the data dynamic update [5, 6], the privacy protection of user's data [7, 8], the data sharing among multiple clients [9, 10] and the multicopy of cloud data [11, 12].

## **Literature Survey**

### **Efficient Remote Data Integrity checking in Critical Information Infrastructures**

Checking data possession in networked information systems such as those related to critical infrastructures (power facilities, airports, data vaults, defense systems, etc.) is a matter of crucial importance. Remote data possession checking protocols permit to check that a remote server can access an uncorrupted file in such a way that the verifier does not need to know beforehand the entire file that is being verified. Unfortunately, current protocols only allow a limited number of successive verifications or are impractical from the computational point of view. In this paper, we present a new remote data possession checking protocol such that: 1) it allows an unlimited number of file integrity verifications; 2) its maximum running time can be chosen at set-up time and traded off against storage at the verifier. Cloud computing is the long dreamed vision of computing as a utility, where data owners can remotely store their data in the cloud to enjoy on-demand high-quality applications and services from a shared pool of configurable computing resources. While data outsourcing relieves the owners of the burden of local data storage and maintenance, it also eliminates their physical control of storage dependability and security, which traditionally has been expected by both enterprises and individuals with high service-level requirements.

---

### 3 IMPLEMENTATION STUDY

#### EXISTING SYSTEM:

The problem of user revocation in shared cloud data auditing was considered in Guan et al. proposed a cloud storage auditing scheme for low-power clients based on distinguish ability obfuscation. Identity-based cloud storage auditing schemes were proposed to simplify key management process.

#### Disadvantages:

- The secret key might be exposed due to the weak security sense and/or the low security settings of the client.
- When the key exposure happens, it often cannot be found out at once. The key exposure might be difficult to be found out because the attacker might stop intrusion at once when it gets the client's secret key.

#### Proposed System & algorithm

We investigate how to preserve the security of cloud storage auditing scheme in any time period other than the key-exposure time period when the key exposure happens. We propose a paradigm named strong key-exposure resilient auditing as a practical solution for this problem in this paper.

#### 4.1 Advantages:

- The security of the cloud storage auditing not only earlier than but also later than the key exposure can be preserved.
  - The security proof and the experimental results demonstrate that the proposed scheme is secure and efficient.
-

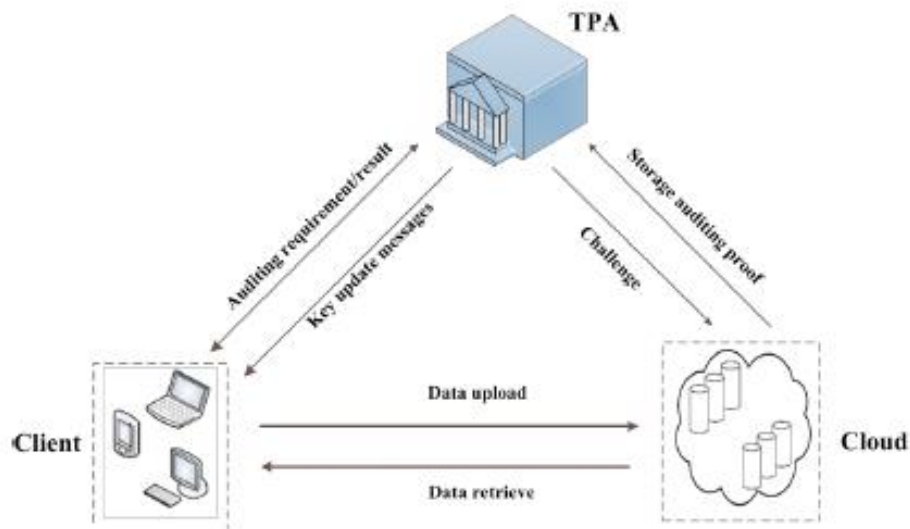


Fig:3.1 System Architecture

## IMPLEMENTATION

### MODULES

- CLIENT
- TPA
- CLOUD SERVER

#### CLIENT:

File owner will register with application and registration details are sent to TPA for verification after verification is successful client can login with username and password and upload files to cloud server by selecting users from list to whom he wants to give access permissions for that file. Client will check for key update messages from TPA for updating key for old file. Client can view uploaded files and view files to which he wants to update key. Considering client as owner and user in user case user can request for decryption key from cloud server. When user receives decryption, he can download shared files from owner.

#### TPA:

TPA can login with valid user name and password. TPA is a trusted party responsible for setting up the authentication process for clients and responding to the

clients 'registration, and also allows the registered clients update keys for every file client uploaded to cloud on time bases by sending message to client with updating message.

TPA will verify request received from cloud server and verify if requested client has permission to download and if that is valid then TPA send challenge to cloud for key update before sending to file requested client.

## 5 RESULTS AND DISCUSSION

### SCREEN SHOTS

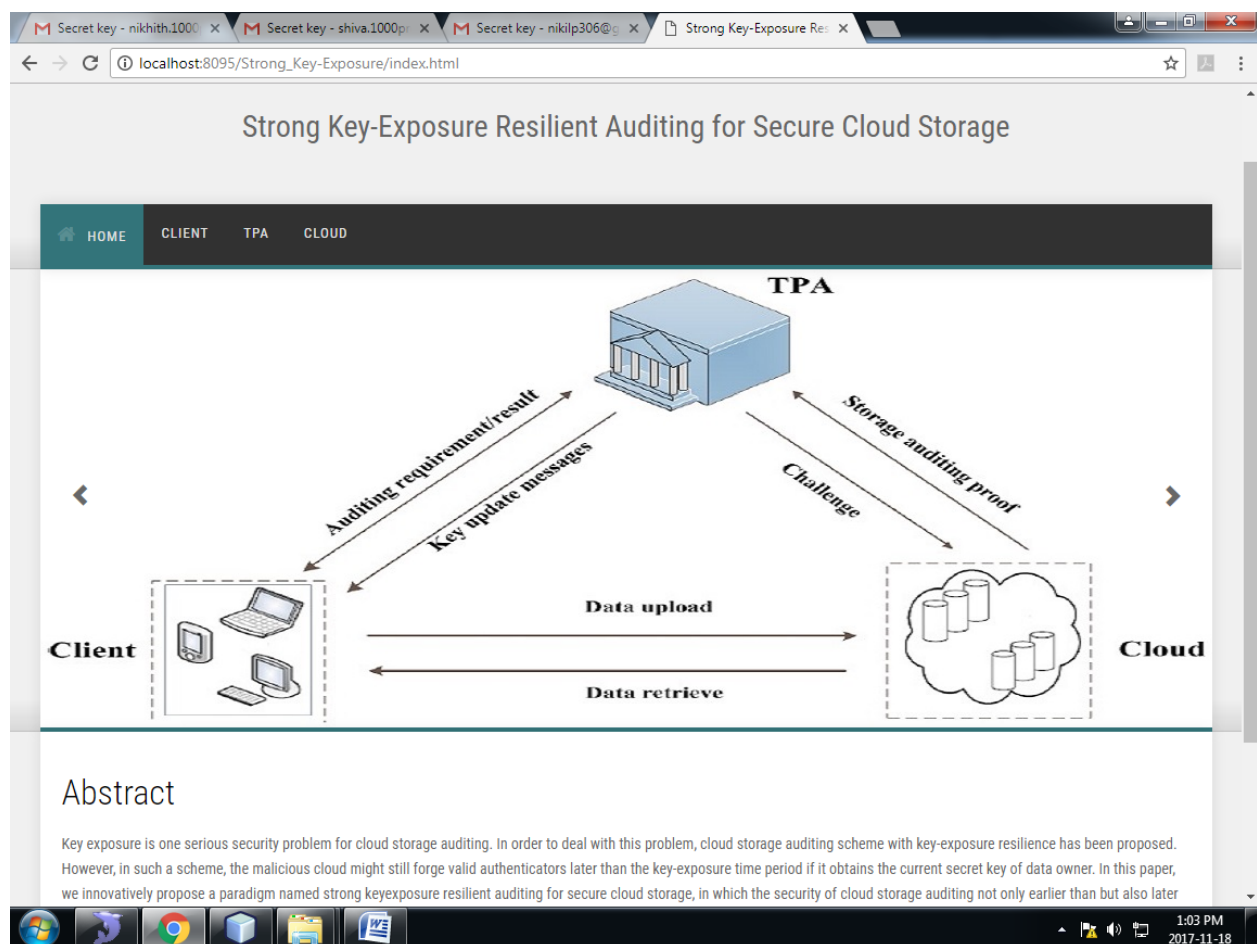


Fig: Home Page

Client Registration Form

User Name

Password

Email Address

Date Of Birth

Select Gender

Address

Mobile Number

Developed By 1000Projects

1:03 PM  
2017-11-18

Fig: client registration



Fig: Client Login

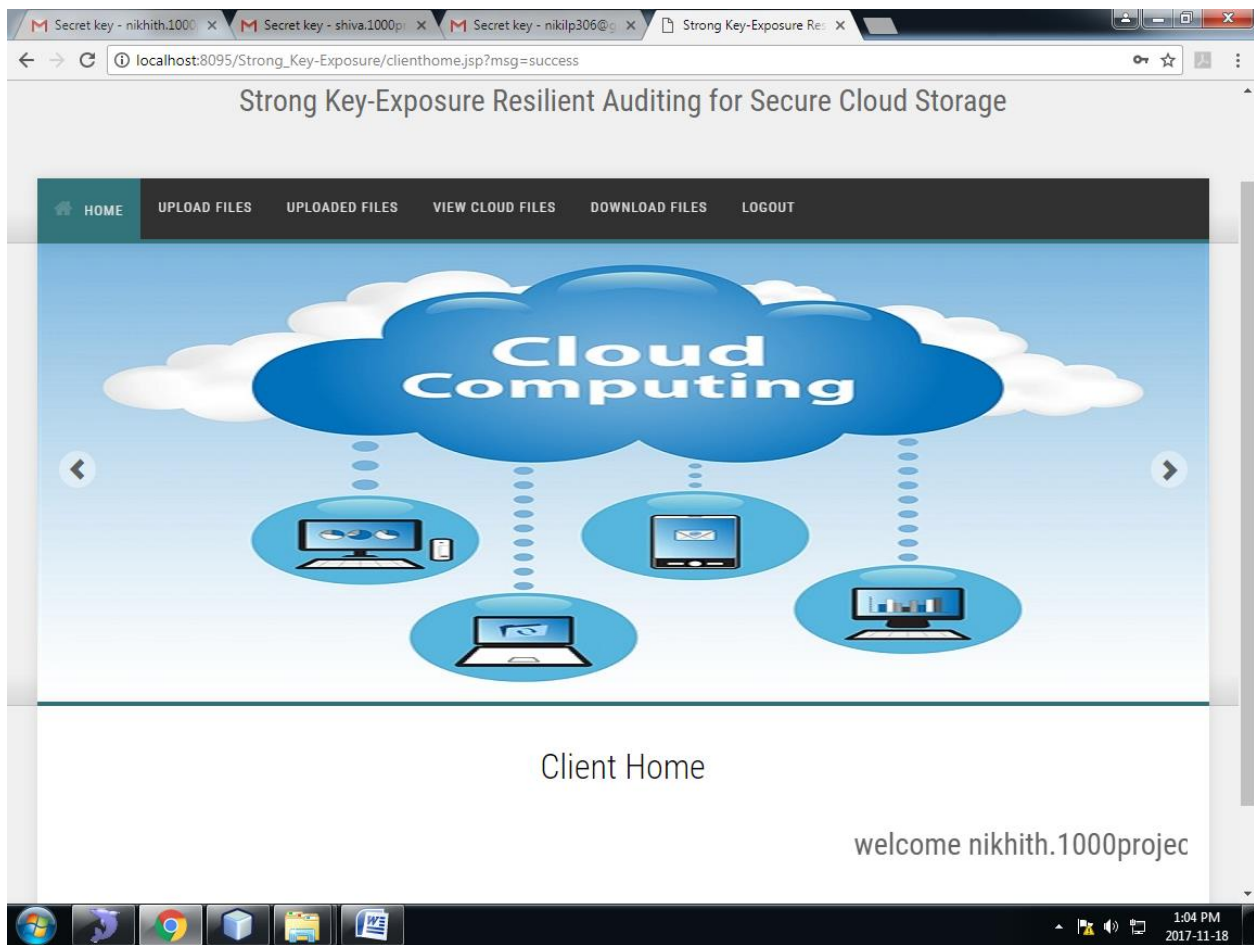


Fig: Client home



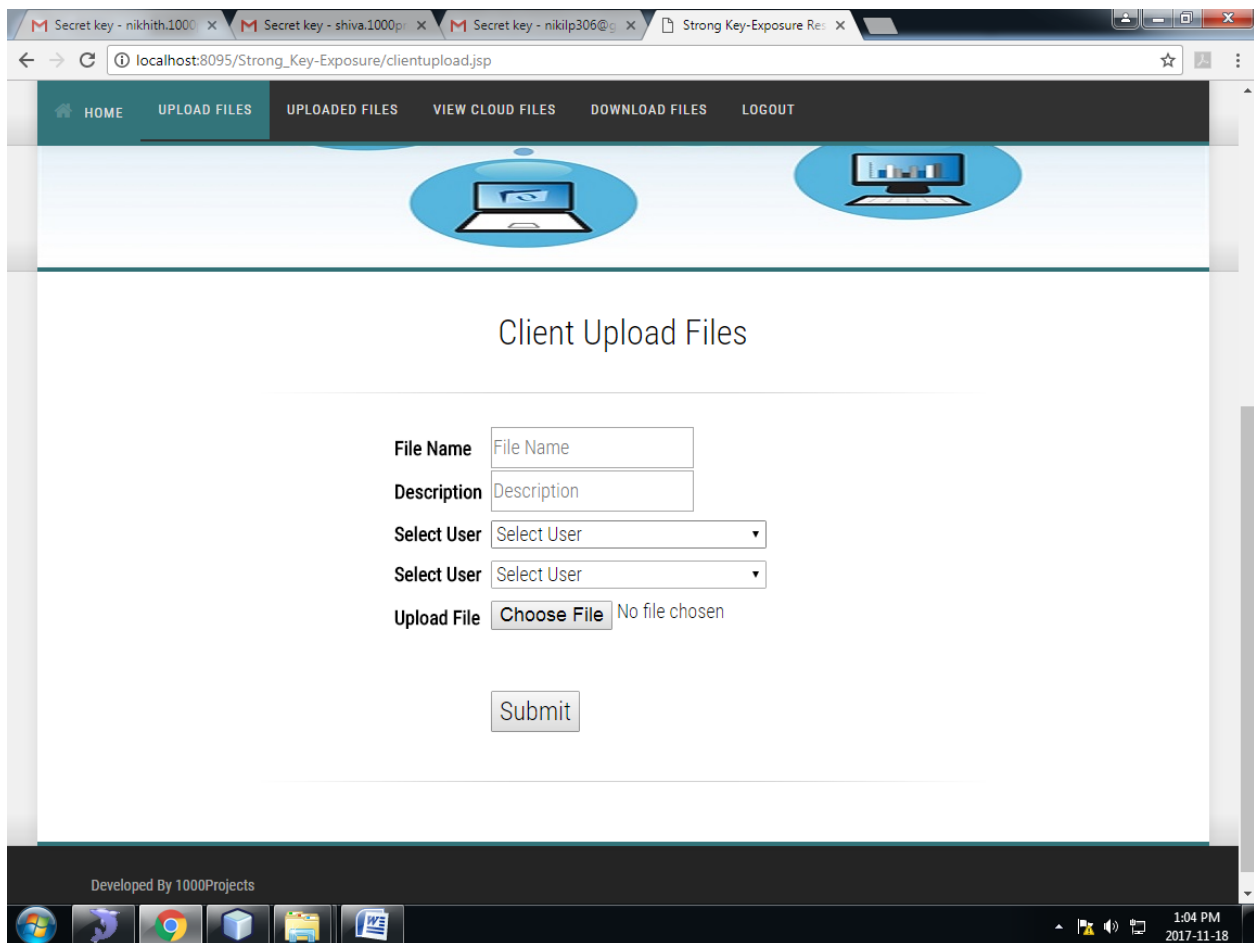


Fig: file Upload

The screenshot shows a web browser window with multiple tabs. The active tab is 'Strong Key-Exposure Res:'. The address bar shows 'localhost:8095/Strong\_Key-Exposure/clientviewfiles.jsp'. The web application has a navigation bar with links: HOME, UPLOAD FILES, **UPLOADED FILES**, VIEW CLOUD FILES, DOWNLOAD FILES, and LOGOUT. Below the navigation bar is a banner image with the word 'Computing' and icons of various devices connected to a cloud. The main content area is titled 'View Uploaded Files' and contains a table with the following data:

File Name	Description	Secret key	Owner	Key Updated Time	Update Key
decryption.txt	decryption	fR4G+XJ/0y9PhlJs1jsFw==	nikhith.1000projects@gmail.com	2017/11/18 12:40:41	Update Key
encryption.txt	encryption	5uhgSxomlLKzA5LhZRSZnA==	nikhith.1000projects@gmail.com	2017/11/18 12:40:51	Update Key

At the bottom of the web application, it says 'Developed By 1000Projects'. The Windows taskbar at the bottom shows the time as 1:04 PM on 2017-11-18.

Fig: Uploaded Files



The screenshot displays a web browser window with multiple tabs. The active tab shows a web application running on localhost:8095. The application has a navigation bar with links: HOME, UPLOAD FILES, UPLOADED FILES, VIEW CLOUD FILES (selected), DOWNLOAD FILES, and LOGOUT. Below the navigation bar is a banner image with the word 'Computing' and a diagram of a cloud connected to various devices. The main content area is titled 'View Uploaded Files' and contains a table with the following data:

File Name	Description	Secret key	Owner	Uploaded Date	Request
decryption.txt	decryption	fR4G+X.J/0y9PhlJs1jsFw==	nikhith.1000projects@gmail.com	2017/11/18 12:40:41	Request
encryption.txt	encryption	5uhgSxomLLKzA5LhZRSZnA==	nikhith.1000projects@gmail.com	2017/11/18 12:40:51	Request

At the bottom of the application, it says 'Developed By 1000Projects'. The Windows taskbar at the bottom shows the time as 1:04 PM on 2017-11-18.

Fig: View Cloud Files

View Uploaded Files

File Name	Description	Key Updated Date	Owner	Download
decryption.txt	decryption	2017/11/18 12:40:41	nikhith.1000projects@gmail.com	Download
encryption.txt	encryption	2017/11/18 12:40:51	nikhith.1000projects@gmail.com	Download
decryption.txt	decryption	2017/11/18 12:40:41	nikhith.1000projects@gmail.com	Download
decryption.txt	decryption	2017/11/18 12:40:41	nikhith.1000projects@gmail.com	Download

Developed By 1000Projects

Fig: Download Files



Fig: TPA Login

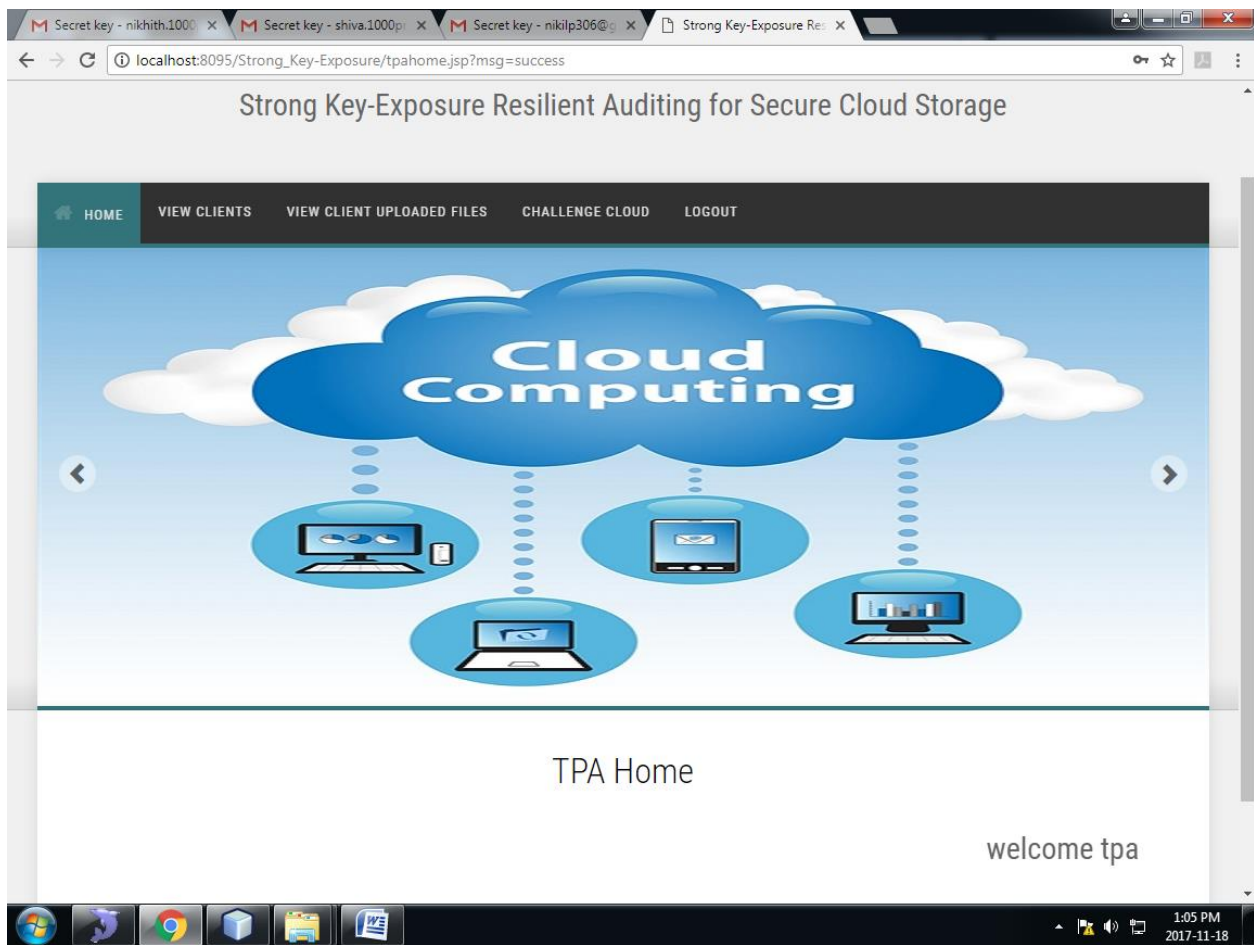


Fig: TPA Home

The screenshot shows a web browser window with multiple tabs. The active tab is titled 'Strong Key-Exposure Res' and the address bar shows 'localhost:8095/Strong\_Key-Exposure/tpaviewclient.jsp'. The web application has a navigation bar with links: HOME, VIEW CLIENTS (active), VIEW CLIENT UPLOADED FILES, CHALLENGE CLOUD, and LOGOUT. Below the navigation bar is a banner with the word 'Computing' in a blue cloud, connected by dotted lines to icons of a desktop monitor, a tablet, and a laptop. The main content area is titled 'View Client Details' and contains a table with client information.

Name	Email	DOB	Gender	Address	Contact No	Status	Activate
dileep	nikilp306@gmail.com	2007-10-29	MALE	1000projects	9052016340	Activated	Activate
nikith	nikhith.1000projects@gmail.com	1995-09-29	MALE	1000projects,Hyderabad	9052016340	Activated	Activate
shiva	shiva.1000projects@gmail.com	2001-12-30	MALE	1000projects,Hyderabad	9052016340	Activated	Activate
ramu	ramu.1000projects@gmail.com	1992-12-28	MALE	1000projects,Hyderabad	9052016340	Activated	Activate

The Windows taskbar at the bottom shows the system clock as 1:05 PM on 2017-11-18.

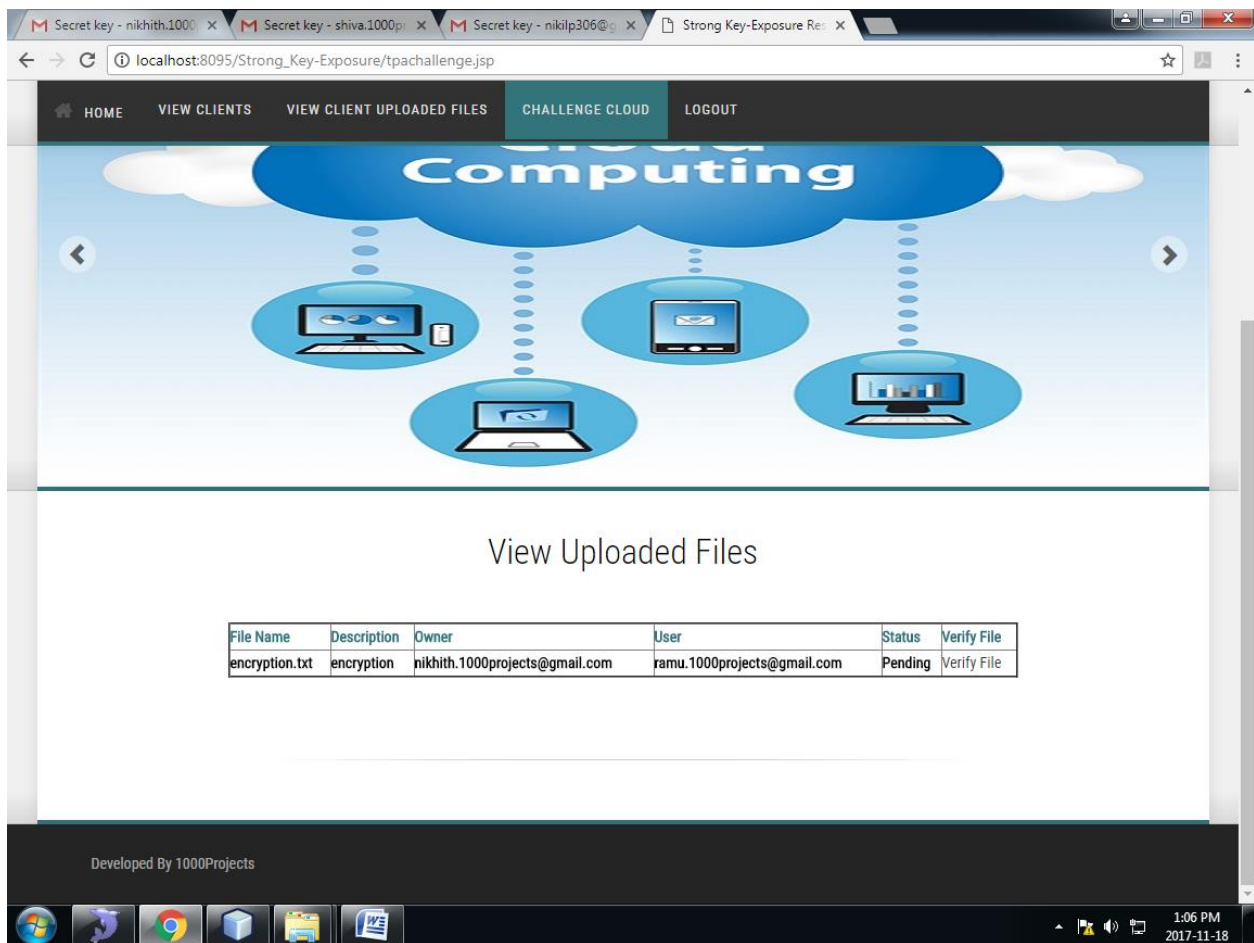
Fig: View Client details

The screenshot shows a web browser window with multiple tabs. The active tab is 'Strong Key-Exposure Res'. The address bar shows 'localhost:8095/Strong\_Key-Exposure/tpaviewfiles.jsp'. The web application has a dark navigation bar with links: HOME, VIEW CLIENTS, VIEW CLIENT UPLOADED FILES (highlighted), CHALLENGE CLOUD, and LOGOUT. Below the navigation bar is a banner image with the word 'Computing' and icons of various devices connected to a cloud. The main content area is titled 'View Client File Details' and contains a table with file information. At the bottom of the page, it says 'Developed By 1000Projects'. The Windows taskbar at the bottom shows the time as 1:06 PM on 2017-11-18.

File Name	Description	Secret key	Owner	Uploaded Date	Send Message
decryption.txt	decryption	fR4G+XJ/0y9PhTJs1jsFw==	nikhith.1000projects@gmail.com	2017/11/18 12:40:41	Send Message
encryption.txt	encryption	5uhgSxomlKzA5LhZRSZnA==	nikhith.1000projects@gmail.com	2017/11/18 12:40:51	Send Message

Fig: View Client file Details





The screenshot displays a web browser window with multiple tabs. The active tab shows a web application titled 'Strong Key-Exposure Res' at the URL 'localhost:8095/Strong\_Key-Exposure/tpachallenge.jsp'. The application has a navigation bar with links: HOME, VIEW CLIENTS, VIEW CLIENT UPLOADED FILES, CHALLENGE CLOUD (highlighted), and LOGOUT. Below the navigation bar is a banner for 'Cloud Computing' featuring a blue cloud and several laptops connected by dotted lines. The main content area is titled 'View Uploaded Files' and contains a table with the following data:

File Name	Description	Owner	User	Status	Verify File
encryption.txt	encryption	nikhith.1000projects@gmail.com	ramu.1000projects@gmail.com	Pending	<a href="#">Verify File</a>

At the bottom of the application, it says 'Developed By 1000Projects'. The Windows taskbar at the bottom shows the time as 1:06 PM on 2017-11-18.

Fig: Verify File

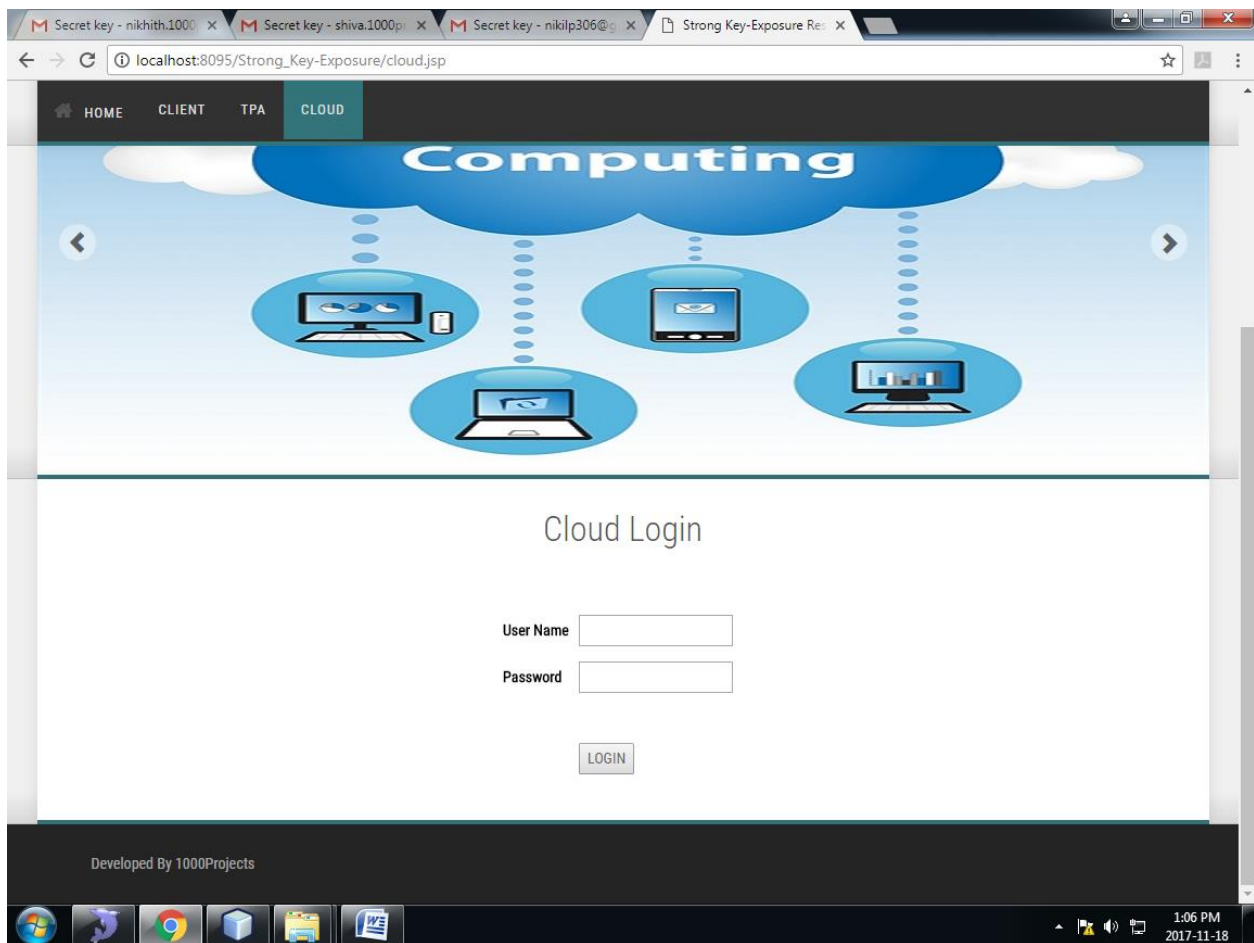


Fig: Cloud Login



The screenshot displays a web browser window with multiple tabs. The active tab shows a web application at `localhost:8095/Strong_Key-Exposure/cloudviewfiles.jsp`. The application has a navigation bar with links: HOME, VIEW CLOUD FILES (selected), VIEW CLIENT REQUESTS, VIEW TPA CHALLENGE, and LOGOUT. Below the navigation bar is a banner image with the word 'Computing' and a diagram of a cloud connected to various devices. The main content area is titled 'View Uploaded Files' and contains a table with the following data:

File Name	Description	Secret key	Owner	Key Updated Time
decryption.txt	decryption	fR4G X.J/0y9PhtJJs1jsFw==	nikhith.1000projects@gmail.com	2017/11/18 12:40:41
encryption.txt	encryption	SuhgSxomlLKzA5LhZRSZnA==	nikhith.1000projects@gmail.com	2017/11/18 12:40:51

The footer of the application states 'Developed By 1000Projects'. The Windows taskbar at the bottom shows the system clock as 1:06 PM on 2017-11-18.

Fig: Cloud Files

The screenshot shows a web browser window with multiple tabs. The active tab is 'Strong Key-Exposure Res'. The URL bar shows 'localhost:8095/Strong\_Key-Exposure/cloudviewrequests.jsp'. The application has a navigation bar with links: HOME, VIEW CLOUD FILES, VIEW CLIENT REQUESTS (active), VIEW TPA CHALLENGE, and LOGOUT. Below the navigation bar is a decorative header with icons of a desktop, a laptop, and a tablet. The main content area is titled 'View Client Requests' and contains a table with 6 columns: File Name, Description, Owner, User, Status, and Forward. The table lists 6 rows of data. At the bottom of the application, it says 'Developed By 1000Projects'. The Windows taskbar at the bottom shows the time as 1:07 PM on 2017-11-18.

File Name	Description	Owner	User	Status	Forward
decryption.txt	decryption	nikhith.1000projects@gmail.com	shiva.1000projects@gmail.com	Updated	Forward
encryption.txt	encryption	nikhith.1000projects@gmail.com	shiva.1000projects@gmail.com	Updated	Forward
encryption.txt	encryption	nikhith.1000projects@gmail.com	ramu.1000projects@gmail.com	forward to TPA	Forward
decryption.txt	decryption	nikhith.1000projects@gmail.com	ramu.1000projects@gmail.com	Updated	Forward
encryption.txt	encryption	nikhith.1000projects@gmail.com	ramu.1000projects@gmail.com	forward to TPA	Forward
decryption.txt	decryption	nikhith.1000projects@gmail.com	nikilp306@gmail.com	Updated	Forward

Fig: View Client requests



Fig: View TPA Challenge

## 6. CONCLUSION AND FUTURE WORK

### CONCLUSION

In this Project, we further study on how to deal with the key exposure problem in cloud storage auditing. We propose a new paradigm called strong key-exposure resilient auditing scheme for secure cloud storage. In this paradigm, the security of the cloud storage auditing not only earlier than but also later than the key exposure can be preserved. We formalize the definition and the security model of this new kind of cloud storage auditing and design a concrete scheme. The security proof and the experimental results demonstrate that the proposed scheme is secure and efficient.

## 7. REFERENCES

- [1] F. Sebe, J. Domingo-Ferrer, A. Martinez-ballets, Y. Deswarte, and J. Quisquater, "Efficient Remote Data Integrity checking in Critical Information Infrastructures," *IEEE Transactions on Knowledge and Data Engineering*, vol. 20, no. 8, pp. 1-6, 2008.
  - [2] C. Wang, K. Ren, W. Lou, and J. Li, "Toward Publicly Auditable Secure Cloud Data Storage Services," *IEEE Network*, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.
  - [3] Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu, and S. S. Yau, "Efficient Provable Data Possession for Hybrid Clouds," *Proc. 17th ACM Conference on Computer and Communications Security*, pp. 756-758, 2010.
  - [4] K. Yang and X. Jia, "Data Storage Auditing Service in Cloud Computing: Challenges, Methods and opportunities," *World Wide Web*, vol. 15, no. 4, pp. 409-428, 2012.
  - [5] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," *IEEE Trans. Parallel and Distributed Systems*, vol. 22, no. 5, pp. 847-859, May 2011.
  - [6] Y. Zhu, H.G. Ahn, H. Hu, S.S. Yau, H.J. An, and C.J. Hu, "Dynamic Audit Services for Outsourced Storages in Clouds," *IEEE Trans. on Services Computing*, vol. 6, no. 2, pp. 409-428, 2013.
  - [7] C. Wang, S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," *IEEE Trans. Computers*, Vol. 62, No. 2, pp. 362-375, 2013.
  - [8] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," *IEEE Trans. Parallel and Distributed Systems*, Vol. 24, No. 9, pp. 1717-1726, 2013.
  - [9] J. Yuan and S. Yu, "Public Integrity Auditing for Dynamic Data Sharing with Multiuser Modification," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1717-1726, Aug. 2015.
  - srevocation in the cloud," *INFOCOM 2013 Proceedings IEEE*, pp. 2904-2912, 2013.
-