



**IJIRCCCE**

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

**Volume 10, Issue 4, April 2022**

**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA

**Impact Factor: 8.165**

 9940 572 462

 6381 907 438

 [ijircce@gmail.com](mailto:ijircce@gmail.com)

 [www.ijircce.com](http://www.ijircce.com)

# Combined Data User-side and Cloud-Side Access Control for Encrypted Cloud Storing

Nikhil Gaikwad<sup>1</sup>, Akshay Bokhare<sup>2</sup>, Prashant Malse<sup>3</sup>, Prof. Shrishail Patil<sup>4</sup>

UG Student, Bhivarabai Sawant Institute of Technology and Research, Wagholi, Pune, India<sup>1,2,3</sup>

Project Guide, Bhivarabai Sawant Institute of Technology and Research, Wagholi, Pune, India<sup>4</sup>

**ABSTRACT:** In this era of internet, e-commerce is growing by leaps and bounds keeping the growth of brick-and-mortar businesses in the dust. In many cases, brick-and-mortar businesses are resorting to having a counterpart which is internet or e-commerce driven. People in the developed world and a growing number of people in the developing world now use e-commerce websites on a daily basis to make their everyday purchases. Still the proliferation of e-commerce in the underdeveloped world is not that great and there is a lot to desire for. This system outlines different aspects of developing an e-commerce website and the optimum solution to the challenges involved in developing one. It consists of the planning process, which starts with determining the use case, domain modeling and architectural pattern of the web application. The entire development process is primarily divided into two parts: the front-end development and the back end development. The database design is also discussed with an emphasis on its relational connectivity. This no-nonsense method of developing an e-commerce website can be easily replicated and followed in developing e-commerce websites in the developing and underdeveloped countries where computing resources are scarce and expensive because of their socio-economic conditions.

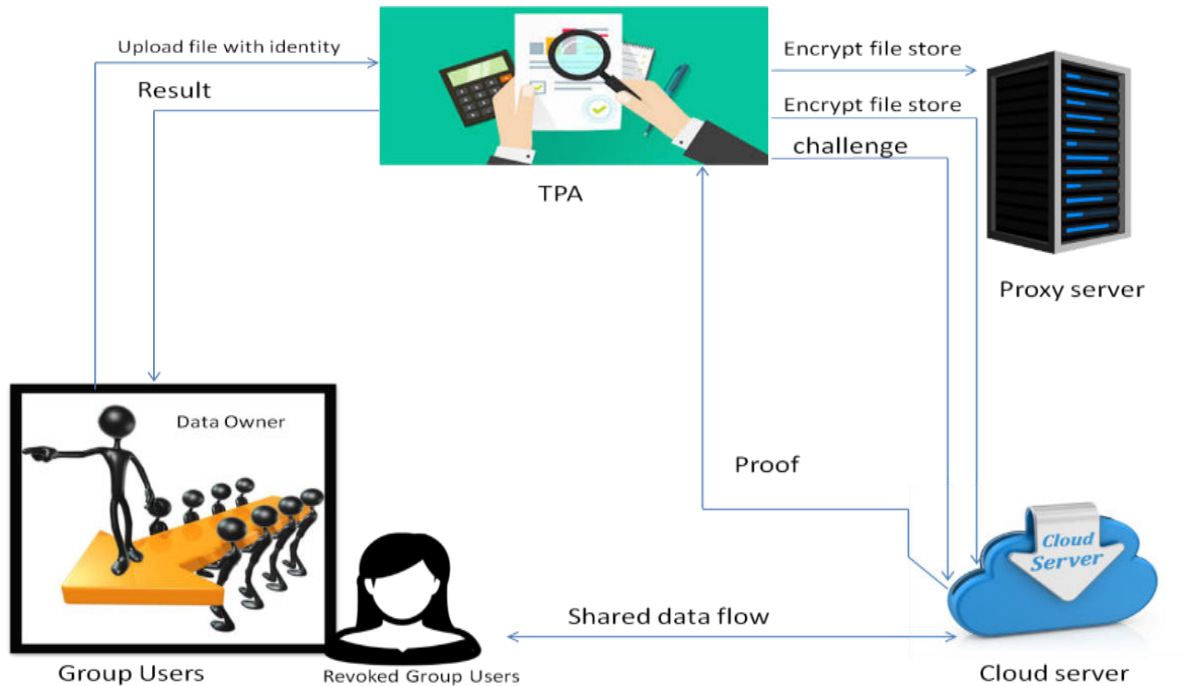
## I. INTRODUCTION

Cloud computing, which has entered considerable attention from exploration communities in academia as well as assiduity, is a distributed calculation model over a large pool of participated-virtualized computing coffers, similar as storehouse, recycling power, operations and services. This kind of new calculation model represents a new vision of furnishing computing services as public serviceability like water and electricity. Pall computing brings a number of benefits for pall druggies. Still, there's a vast variety of walls before pall computing can be extensively stationed. A recent check by Oracle appertained the data source from transnational data pot enterprise panel, showing that security represents 87 of pall druggies' fears<sup>1</sup>. One of the major security enterprises of pall druggies is the integrity of their outsourced lines since they no longer physically retain their data and therefore lose the control over their data. Also, the pall garçon isn't completely trusted and it isn't obligatory for the pall garçon to report data loss incidents. Indeed, to ascertain pall computing trustability, the pall security alliance (CSA) published an analysis of pall vulnerability incidents

## II. MOTIVATION

The Cloud can be used to enable data-sharing capabilities, which can give an abundant number of benefits to the stoner. With multiple druggies from different organisations contributing to data in the Cloud, lower time and plutocrat will be spent, compared with having to manually change data that creates a clutter of spare and conceivably out-of-date documents. Therefore, the Cloud makes data participating with anyone in the world both more accessible and easy. .

### SYSTEM ARCHITECTURE



### III. EXISTING SYSTEM

**Methodology** (Architecture) Remote data integrity checking (RDIC) enables a data storehouse garçon, say a pall garçon, to prove to a verifier that it's actually storing a data proprietor's data actually. To date, a number of RDIC protocols have been proposed in the literature, but utmost of the constructions suffer from the issue of a complex crucial operation, that is, they calculate on the precious public key structure (PKI), which might hamper the deployment of RDIC in practice.

### IV. PROPOSED SYSTEM

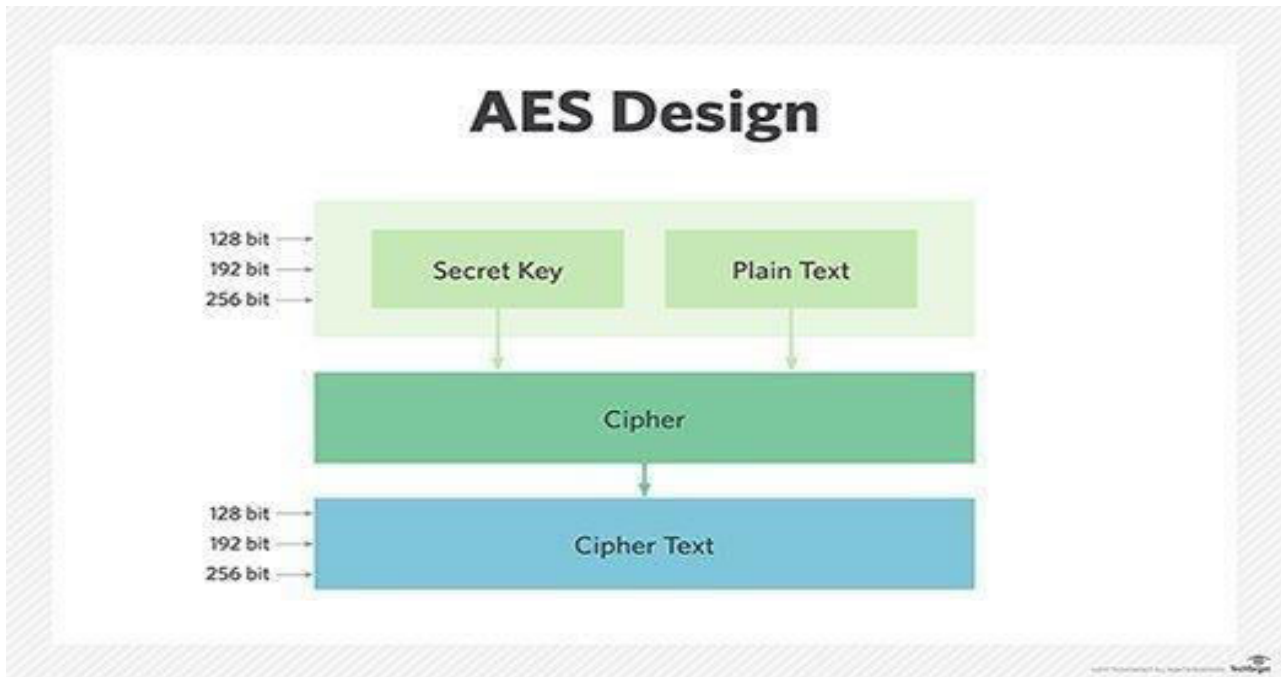
**Methodology** (Architecture) we propose a new construction of identity- grounded (ID- grounded) RDIC protocol by making use of crucial-homomorphic cryptographic primitive to reduce the system complexity and the cost for establishing and managing the public key authentication frame in PKI grounded RDIC schemes. We formalize ID-grounded RDIC and its security model including security against a vicious pall garçon and zero knowledge sequestration against a third- party verifier. The proposed IDgrounded RDIC protocol leaks no information of the stored data to the verifier during the RDIC process.

#### a. ALGORITHM

##### What's AES?

128- bit Advanced Encryption Standard (AES) is used for increase data security and confidentiality. In this proposed approach data is translated using AES and also uploaded on a pall. The AES machine encrypts the plain textbook ( source data) into cipher textbook ( translated data) and sends it to the NAND flash for storehouse. Equally, if the host wants to recoup data from the storehouse device, the AES machine decrypts the cipher textbook in the NAND flash, and also transmits data to the host as plain textbook.

For illustration Cipher Type Symmetric block cipher Symmetric block cipher Block size 64 bits 128 bits Crucial length 56 bits 128/192/256 bits Security Rendered insecure Considered secure



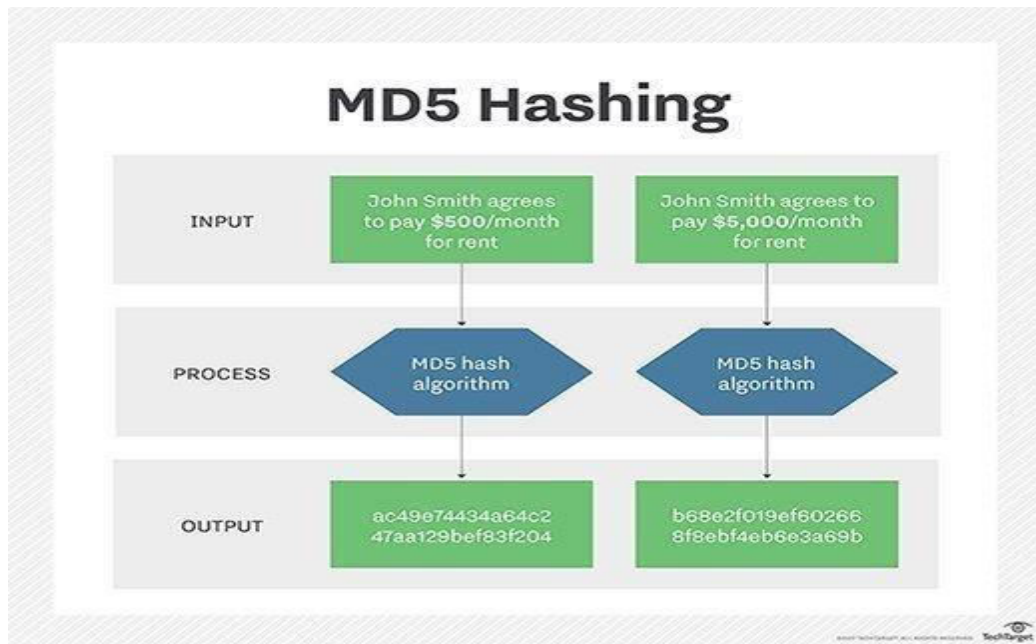
### What's MD5? \*

MD5 is mincing algorithm, a bit like a CRC checksum algo, the data is translated, it's minced, and therefore uncoverable. It's in fact presto to cipher.

Encryption algo are a 2- way system, data can be translated and deciphered with valid key. They generally involve further circles and shifting slower also checksum •

MD5 is most generally used to corroborate the integrity of train. MD5 stands for Message Digest. For illustration For illustration, if we've a list of words of English and we want to check if a given word is in the list, it would be hamstrung to consecutively compare the word with all particulars until we find a match.





### A. ADVANTAGES AND DISADVANTAGES

To reduce the system complexity.

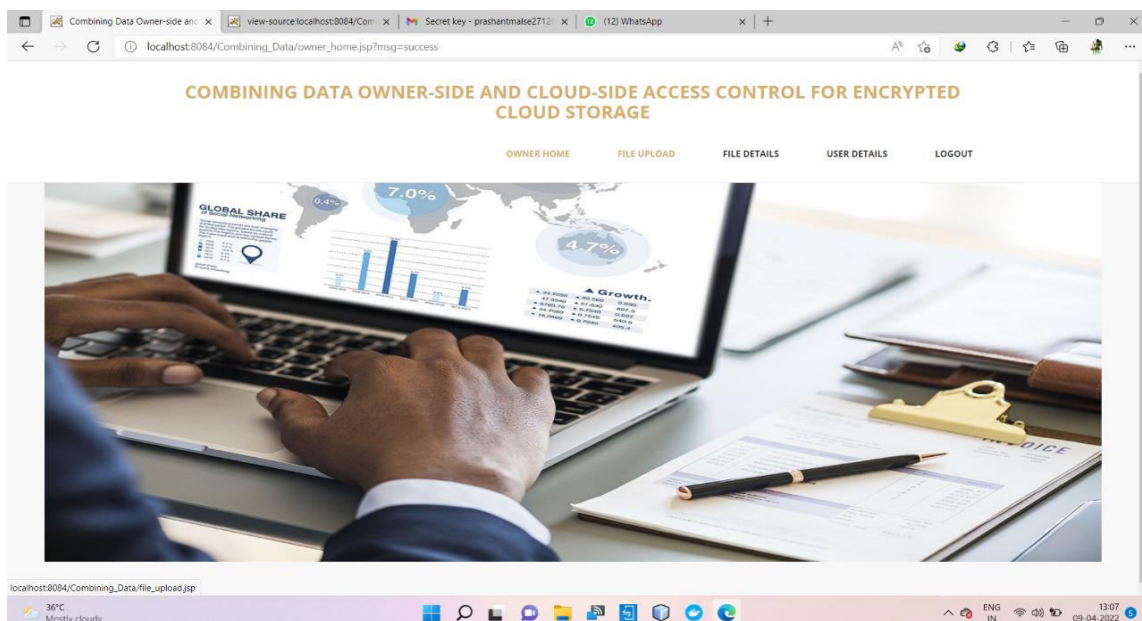
The cost for establishing and managing the public key authentication frame in PKI grounded RDIC schemes. Leaks no information of the stored data to the verifier during the RDIC process.

### B. OPERATIONS

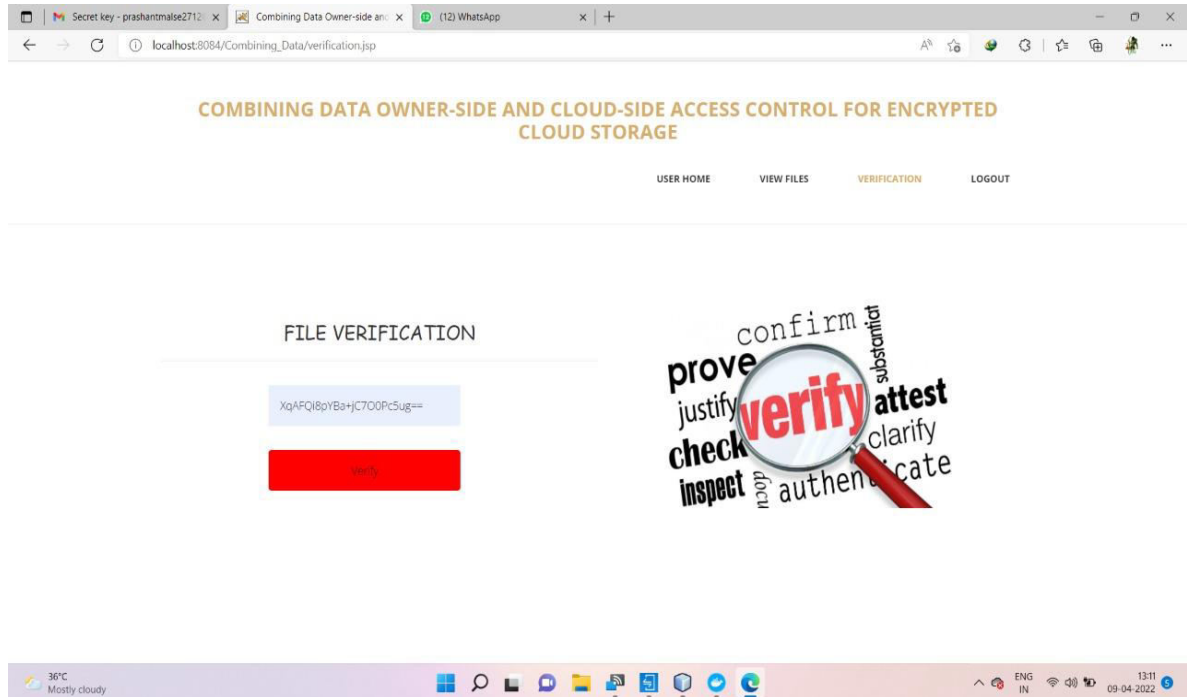
The use of encryption to keep data nonpublic is generally combined with integrity protection Data Stored in Drive.

## IV. RESULTS AND DISCUSSIONS

### 1) Home Page

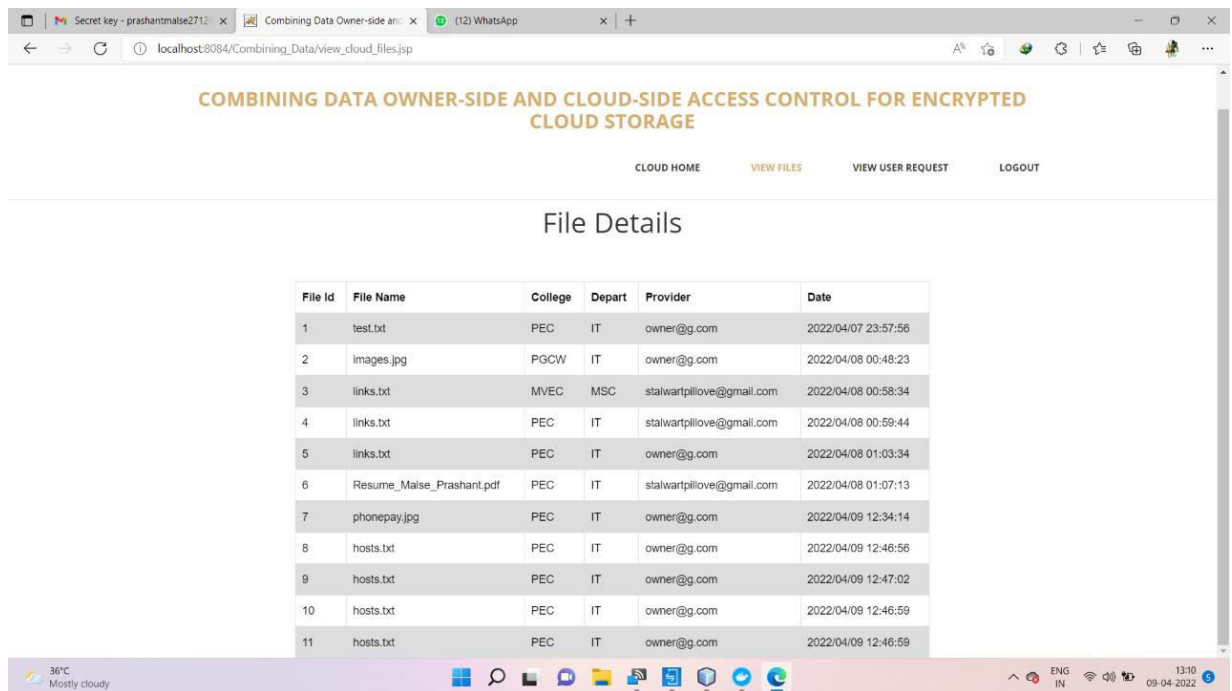


## 2) File Verification



The screenshot shows a web browser window with the URL `localhost:8084/Combining_Data/verification.jsp`. The page title is "COMBINING DATA OWNER-SIDE AND CLOUD-SIDE ACCESS CONTROL FOR ENCRYPTED CLOUD STORAGE". The navigation menu includes "USER HOME", "VIEW FILES", "VERIFICATION" (highlighted), and "LOGOUT". The main content area is titled "FILE VERIFICATION" and contains a text input field with the value `XqAFQI8pYBa+JC700PcSug==` and a red "Verify" button. To the right of the interface is a graphic with a magnifying glass over the word "verify" and other related terms like "confirm", "prove", "justify", "check", "inspect", "substantiate", "attest", "clarify", "authenticate", and "validate". The Windows taskbar at the bottom shows the date as 09-04-2022 and the time as 13:11.

## 3) Files Details

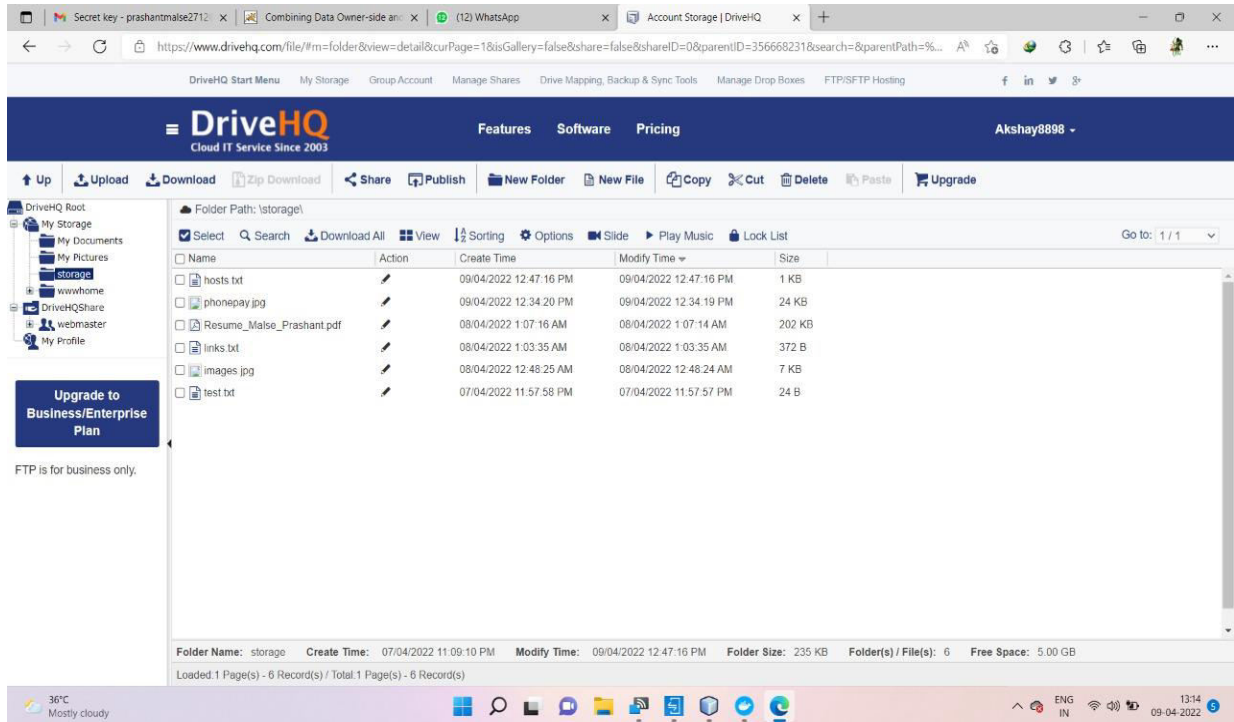


The screenshot shows a web browser window with the URL `localhost:8084/Combining_Data/view_cloud_files.jsp`. The page title is "COMBINING DATA OWNER-SIDE AND CLOUD-SIDE ACCESS CONTROL FOR ENCRYPTED CLOUD STORAGE". The navigation menu includes "CLOUD HOME", "VIEW FILES", "VIEW USER REQUEST", and "LOGOUT". The main content area is titled "File Details" and contains a table with the following data:

File Id	File Name	College	Depart	Provider	Date
1	tes.txt	PEC	IT	owner@g.com	2022/04/07 23:57:56
2	images.jpg	PGCW	IT	owner@g.com	2022/04/08 00:48:23
3	links.txt	MVEC	MSC	stalwartpillove@gmail.com	2022/04/08 00:58:34
4	links.txt	PEC	IT	stalwartpillove@gmail.com	2022/04/08 00:59:44
5	links.txt	PEC	IT	owner@g.com	2022/04/08 01:03:34
6	Resume_Maise_Prashant.pdf	PEC	IT	stalwartpillove@gmail.com	2022/04/08 01:07:13
7	phonepay.jpg	PEC	IT	owner@g.com	2022/04/09 12:34:14
8	hosts.txt	PEC	IT	owner@g.com	2022/04/09 12:46:56
9	hosts.txt	PEC	IT	owner@g.com	2022/04/09 12:47:02
10	hosts.txt	PEC	IT	owner@g.com	2022/04/09 12:46:59
11	hosts.txt	PEC	IT	owner@g.com	2022/04/09 12:46:59

The Windows taskbar at the bottom shows the date as 09-04-2022 and the time as 13:10.

#### 4) Drive

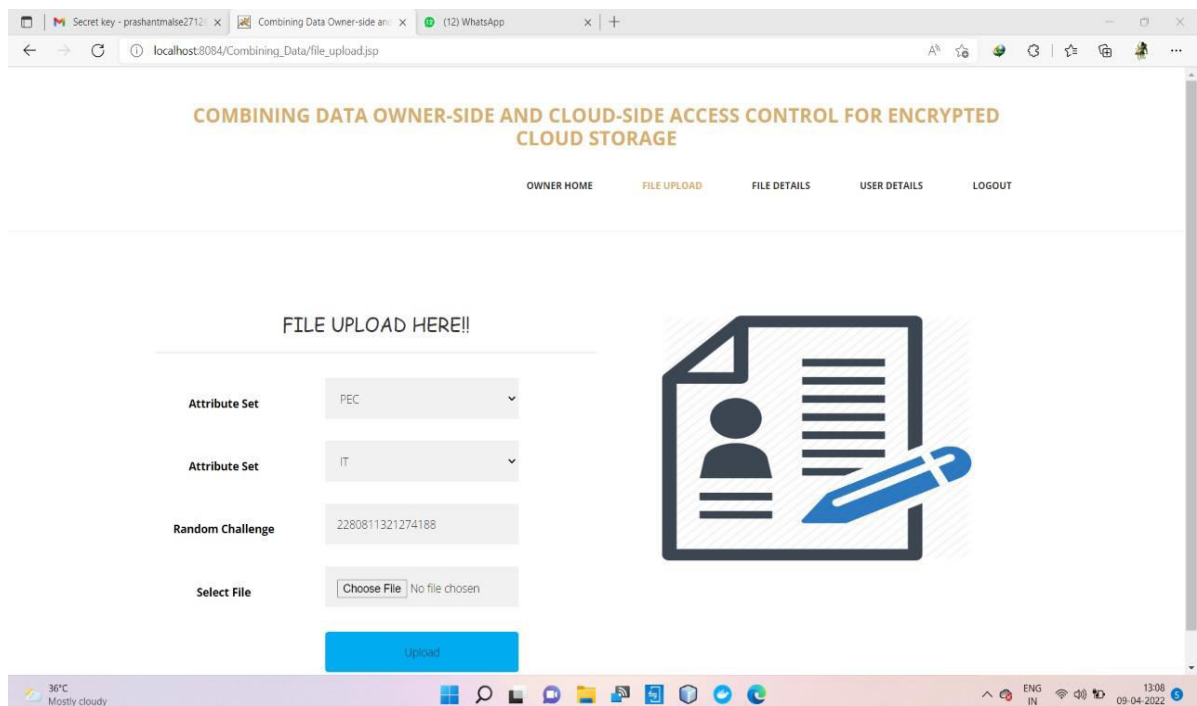


The screenshot shows the DriveHQ web interface. The main content area displays a folder named 'storage' containing the following files:

Name	Action	Create Time	Modify Time	Size
hosts.txt	[Edit]	09/04/2022 12:47:16 PM	09/04/2022 12:47:16 PM	1 KB
phonepay.jpg	[Edit]	09/04/2022 12:34:20 PM	09/04/2022 12:34:19 PM	24 KB
Resume_Maise_Prashant.pdf	[Edit]	08/04/2022 1:07:16 AM	08/04/2022 1:07:14 AM	202 KB
links.txt	[Edit]	08/04/2022 1:03:35 AM	08/04/2022 1:03:35 AM	372 B
images.jpg	[Edit]	08/04/2022 12:48:25 AM	08/04/2022 12:48:24 AM	7 KB
test.txt	[Edit]	07/04/2022 11:57:58 PM	07/04/2022 11:57:57 PM	24 B

Folder Summary: Folder Name: storage, Create Time: 07/04/2022 11:09:10 PM, Modify Time: 09/04/2022 12:47:16 PM, Folder Size: 235 KB, Folder(s) / File(s): 6, Free Space: 5.00 GB.

#### 5) Upload

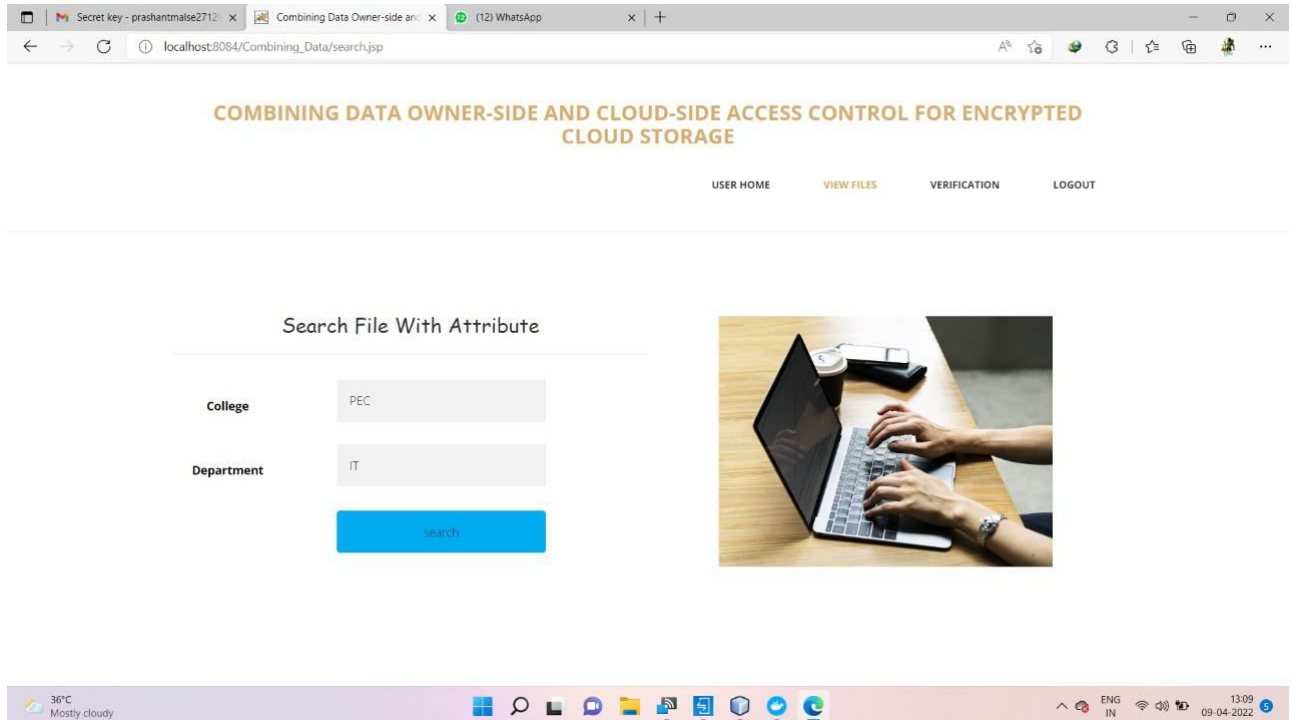


The screenshot shows a web application interface for file upload. The main heading is "COMBINING DATA OWNER-SIDE AND CLOUD-SIDE ACCESS CONTROL FOR ENCRYPTED CLOUD STORAGE". The interface includes a navigation menu with "OWNER HOME", "FILE UPLOAD", "FILE DETAILS", "USER DETAILS", and "LOGOUT".

The "FILE UPLOAD HERE!!" section contains the following fields:

- Attribute Set: PEC (dropdown)
- Attribute Set: IT (dropdown)
- Random Challenge: 2280811321274188
- Select File: Choose File (button) | No file chosen
- Upload (button)

## 6) Search File



## V. CONCLUSION & FUTURE SCOPE

In this, we delved a new primitive called identity- grounded remote data integrity checking for secure pall storehouse. We homogenized the security model of two important parcels of this primitive, videlicet, soundness and perfect data sequestration. We handed a new construction of this primitive and showed that it achieves soundness and perfect data Page 2 of 3 sequestration. Both the numerical analysis and the perpetration demonstrated that the proposed protocol is effective and practical. Extend this work with Group Management with Forward Secrecy & Backward Secrecy by Time Duration & Recovery of Train when Data Integrity Checking Fault Occur.

## REFERENCES

1. K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, no. 1, pp. 69–73, 2020.
2. L. Zhou, Y. Zhu, and A. Castiglione, "Efficient k-NN query over encrypted data in cloud with limited key-disclosure and offline data owner," Computers & Security, vol. 69, pp. 84–96, 2017.
3. S. Hu, Q. Wang, J. Wang, Z. Qin, and K. Ren, "Securing SIFT: Privacy-preserving outsourcing computation of feature extractions over encrypted image data," IEEE Transactions on Image Processing, vol. 25, no. 7, pp. 3411–3425, 2016.
4. H.-M. Sun, Y.-H. Chen, and Y.-H. Lin, "oPass: A user authentication protocol resistant to password stealing and password reuse attacks," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 651–663, 2017.
5. L. Harn and J. Ren, "Generalized digital certificate for user authentication and key establishment for secure communications," IEEE Transactions on Wireless Communications, vol. 10, no. 7, pp. 2372–2379, 2011.
6. L. Zhou, Y. Zhu and A. Castiglione, " Efficient k -NN query over encrypted data in cloud with limited key-disclosure and offline data owner ", Comput. Secur., vol. 69, pp. 84-96, Aug. 2019.
7. S. Hu, Q. Wang, J. Wang, Z. Qin and K. Ren, "Securing SIFT: Privacy-preserving outsourcing computation of feature extractions over encrypted image data", IEEE Trans. Image Process., vol. 25, no. 7, pp. 3411- 3425, Jul. 2016.





8. W. Chansuwath and T. Senivongse, "A model-driven development of web applications using AngularJS framework," 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), 2016, pp. 1-6, doi: 10.1109/ICIS.2016.7550838.
9. Jadhav, M.A., Sawant, B.R. and Deshmukh, A., 2015. Single page application using angularjs. International Journal of Computer Science and Information Technologies, 6(3), pp.2876-2879.



INNO  SPACE  
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

 **doi**<sup>®</sup>  
**cross** **ref**

**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  [ijircce@gmail.com](mailto:ijircce@gmail.com)



[www.ijircce.com](http://www.ijircce.com)

Scan to save the contact details