Efficient Traceable Authorized Search System For Secure Cloud Storage

CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY
INNOVATING TOMORROW
2008
KADAPA (Dt.)

Department Of CSE

M. Karthik	192P1A0569
M. Mahaboob Basha	192P1A0576
P. Bindu Shruthika	192P1A0596
P. Naga Lakshmi	192P1A0595
M.Mahendra Kumar Reddy	192P1A0575

Project Guide	Project Co-ordinator	Head Of Department
Mr. N. Srinivasan	Mr. N. Srinivasan	Mrs. D. Salma Faroze

Contents

- Abstract
- Introduction
- System requirements
  - Hardware requirements
  - Software requirements
- Modules Used
- UML Diagrams
  - Use Case Diagrams
  - Class Diagrams
  - Sequence Diagrams
  - Activity Diagrams
- Screenshots of Results
- Test Cases
- Conclusion
- References & Web Resources

Abstract

- Secure search over encrypted remote data is crucial in cloud computing to guarantee the data privacy and usability. To prevent unauthorized data usage, fine-grained access control is necessary in multi-user system.
- However, authorized user may intentionally leak the secret key for financial benefit. Thus, tracing and revoking the malicious user who abuses secret key needs to be solved imminently.
- We propose an escrow free traceable attribute based multiple keywords subset search system with verifiable outsourced decryption.
- Also, the decryption process only requires ultra lightweight computation, which is a desirable feature for energy-limited devices. In addition, efficient user revocation is enabled after the malicious user is figured out.
- Moreover, the proposed system is able to support flexible number of attributes rather than polynomial bounded. Flexible multiple keyword subset search pattern is realized, and the change of the query keywords order does not affect the search result.

Introduction

- **Network Model :** The system comprises of four entities, namely
  - Key Generation Center (KGC)
  - Cloud Server (CS)
  - Data Owner
  - Data User
- **Generate Secure File And Keyword Model :** In this Model Data Owner extracts a keyword set from the file. Then encrypts the message with secret key using Cryptographic secure symmetric encryption algorithm and generates a verification key that can be used to verify the result of outsourced computing..
- **File Recovery and Verification Model:** The verification key is generated in the Encryption algorithm, which is used to verify the correctness of the transformed cipher text that is generated by the cloud server in the following Test & Transform algorithm. The encrypted files, secure keyword set indexes and verification keys are outsourced to cloud storage.
- **Trace Malicious User Model:** If an authorized use publicly sells or leaks his attribute secret key, then the misbehavior will be discovered. Then the key sanity check algorithm verifies the sanity of the key and the trace algorithm recovers the traitors real identity.

System Requirements

➢ Hardware requirements:

Processor	:	i3 or above
RAM	:	2 GB or more
Hard disk	:	40 GB or more

➢ Software requirements:

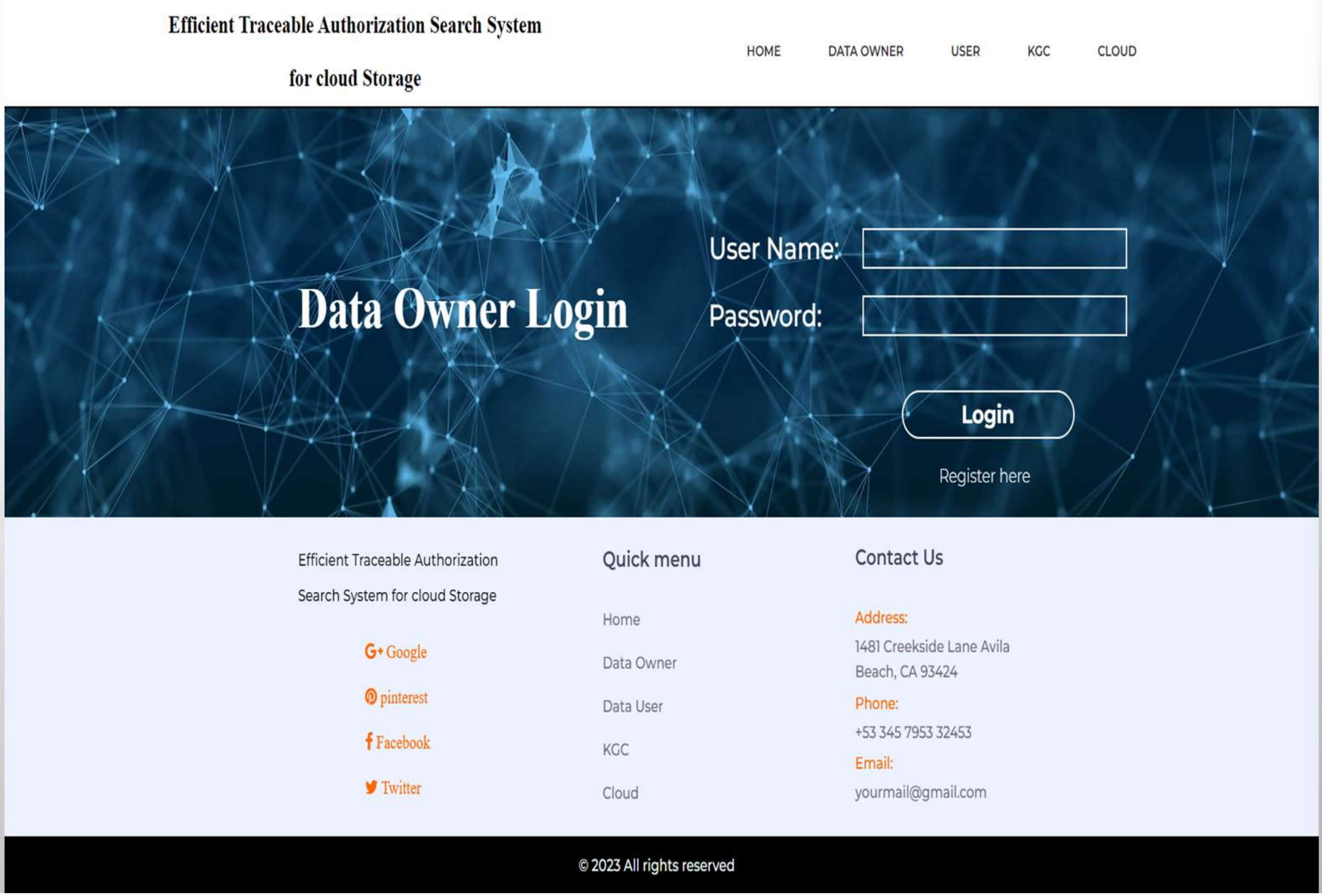
Operating system	:	windows 10 or above
Coding language	:	java/J2EE
Tool	:	netbeans 7.2.1 or above
Database	:	mysql

Modules Used

1. Data Owner
2. Data User
3. Key Generation Centre(KGC)
4. Cloud Secure (CS)

Module – 1 : Data Owner

- Data owner utilizes the cloud storage service to store the files.
- Before the data outsourcing, the data owner extracts keyword set from the file and encrypts it into secure index.
- The document is also encrypted to ciphertext.
- During the encryption process, the access policy is specified and embedded into the ciphertext to realize fine-grained access control.



Efficient Traceable Authorization Search System

for cloud Storage

Data Owner Login

User Name:

Password:

Efficient Traceable Authorization Search System for cloud Storage

Contact Us

Address:
1481 Creekside Lane Avila
Beach, CA 93424

Phone:
+53 345 7953 32453

Email:
yourmail@gmail.com

© 2023 All rights reserved

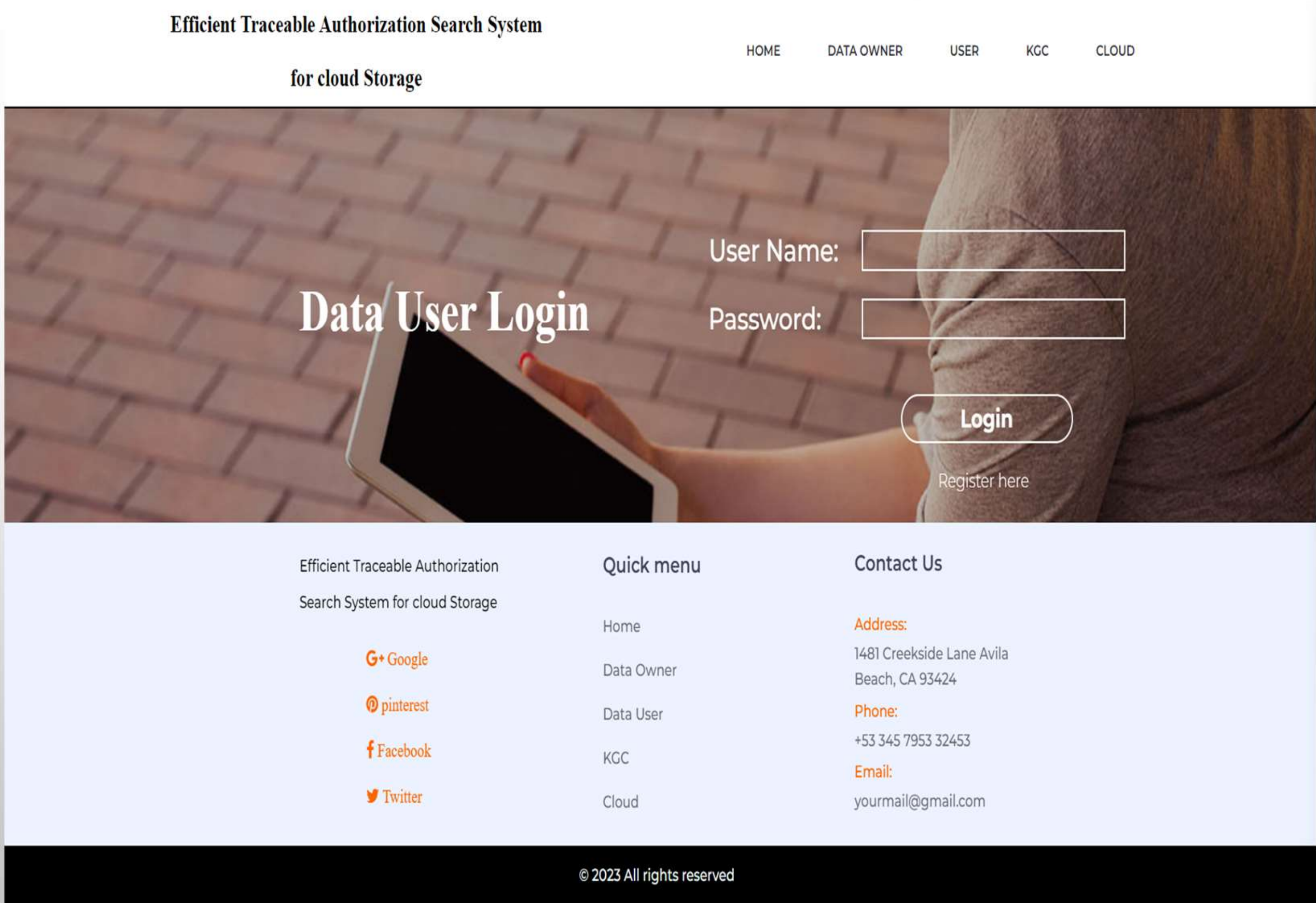
Module – 2 : Data User

- Each data user has attribute set to describe his characteristics, such as professor, computer science college, dean, etc.

- The attribute set is embedded into user's secret key. Using the secret key, data user is able to search on the encrypted files stored in the cloud, i.e., chooses a keyword set that he wants to search.

- Then, the keyword is encrypted to a trapdoor using user's secret key. If the user's attribute set satisfies the access policy defined in the encrypted files, the cloud server responds on user's search query and finds the match files.

- Otherwise, the search query is rejected. After the match files are returned, the user runs decryption algorithm to recover the plaintext.



Efficient Traceable Authorization Search System

for cloud Storage

Data User Login

User Name:

Password:

Efficient Traceable Authorization Search System for cloud Storage

Contact Us

Address:
1481 Creekside Lane Avila
Beach, CA 93424

Phone:
+53 345 7953 32453

Email:
yourmail@gmail.com

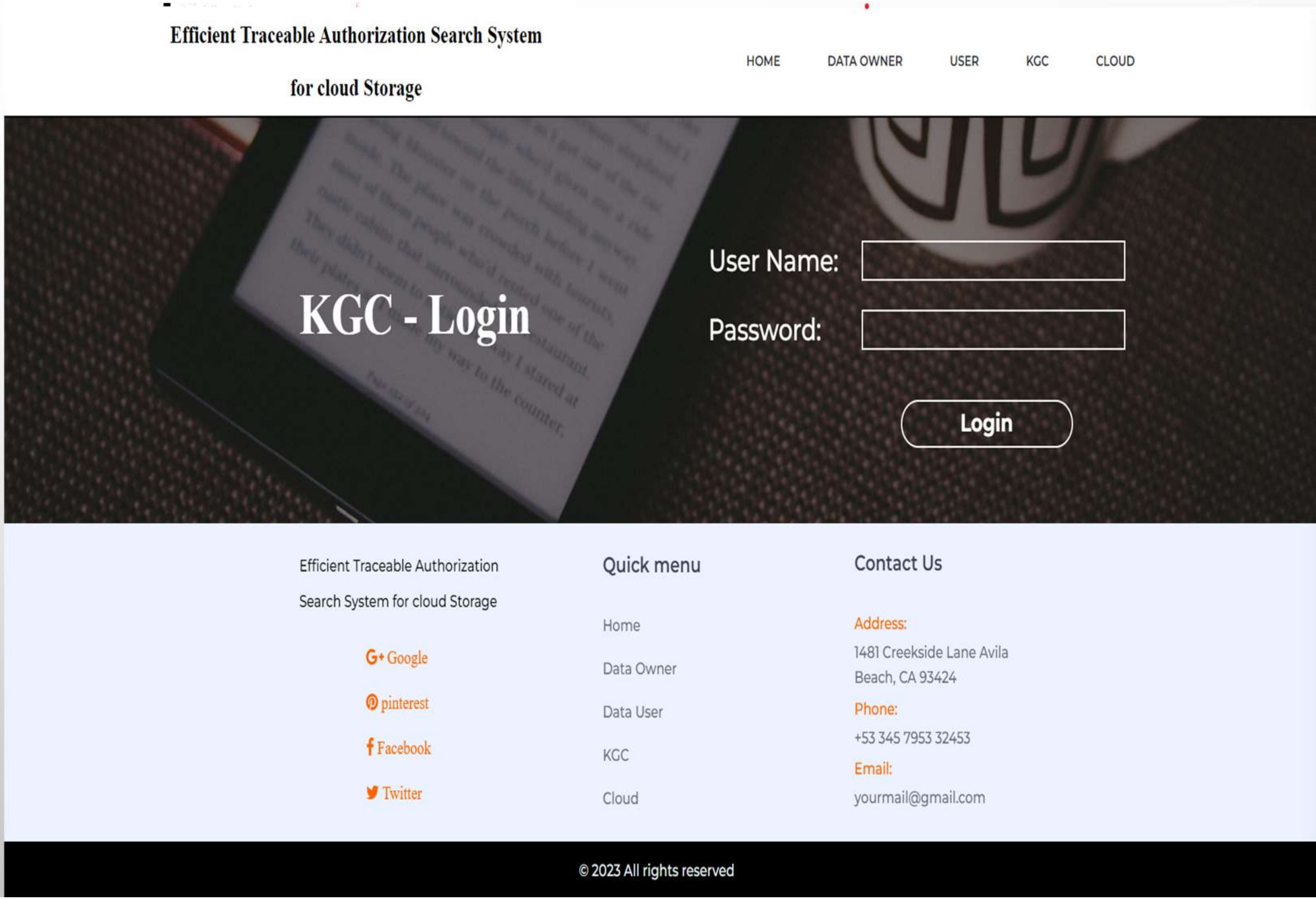
© 2023 All rights reserved

Module – 3 : Key Generation Centre

- KGC is responsible to generate the public parameter for the system and the public/secret key pairs for the users.

- Once the user’s secret key is leaked for profits or other purposes, KGC runs trace algorithm to find the malicious user.

- Once After the traitor is traced, KGC sends user revocation request to cloud server to revoke the user’s search privilege.



Efficient Traceable Authorization Search System

for cloud Storage

KGC - Login

User Name:

Password:

Efficient Traceable Authorization Search System for cloud Storage

Quick menu

Contact Us

Address:
1481 Creekside Lane Avila
Beach, CA 93424

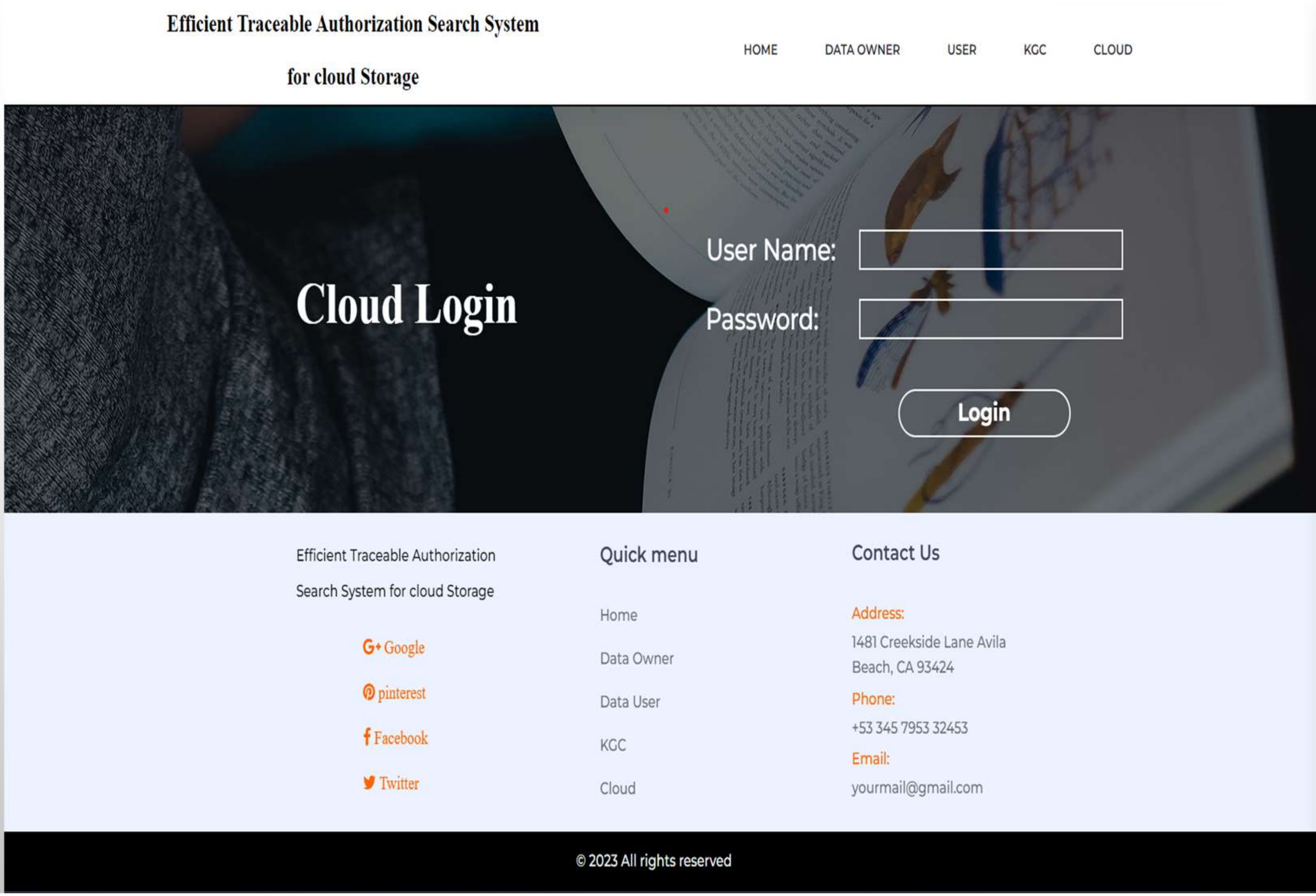
Phone:
+53 345 7953 32453

Email:
yourmail@gmail.com

© 2023 All rights reserved

Module – 4 : Cloud Server

- Cloud server has tremendous storage space and powerful computing capability, which provides on-demand service to the system.
- Cloud server is responsible to store the data owner's encrypted files and respond on data user's search query.



Efficient Traceable Authorization Search System

for cloud Storage

Efficient Traceable Authorization Search System for cloud Storage

Contact Us

Address:
1481 Creekside Lane Avila
Beach, CA 93424

Phone:
+53 345 7953 32453

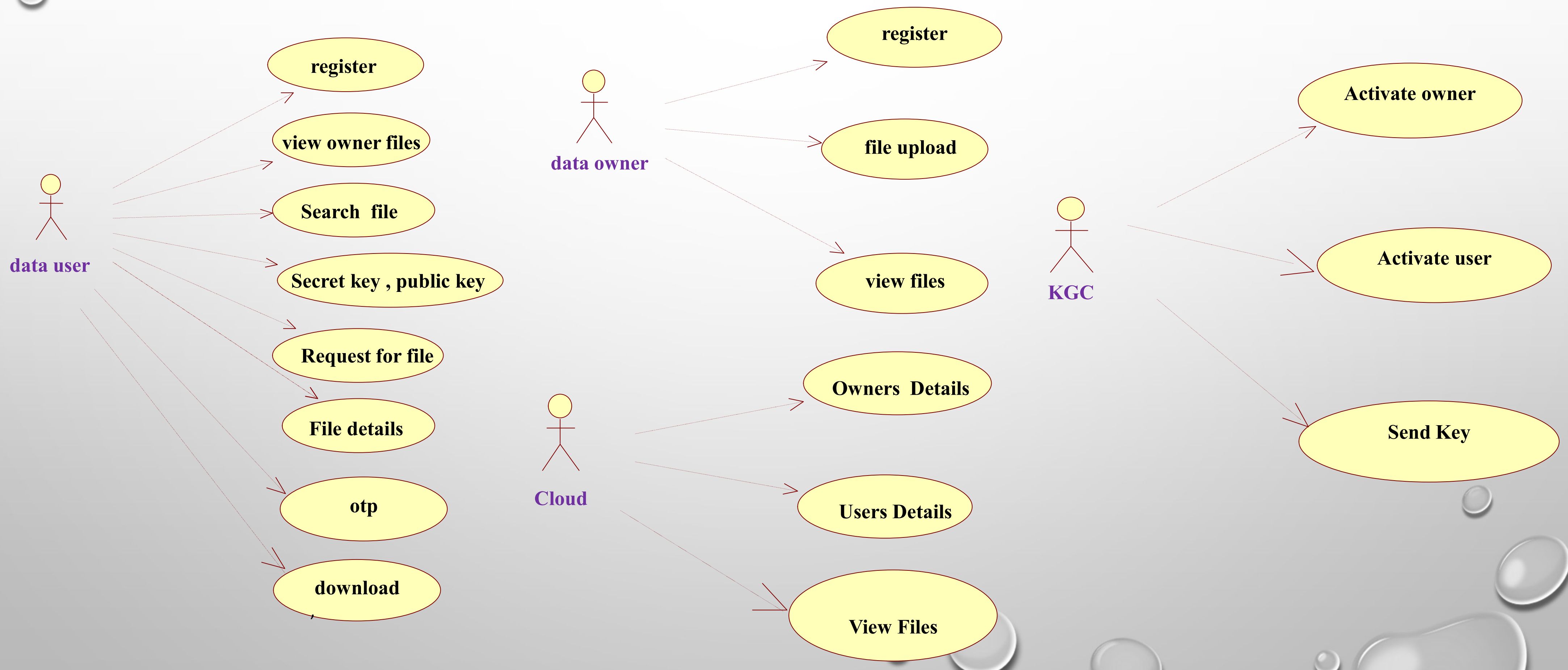
Email:
yourmail@gmail.com

© 2023 All rights reserved

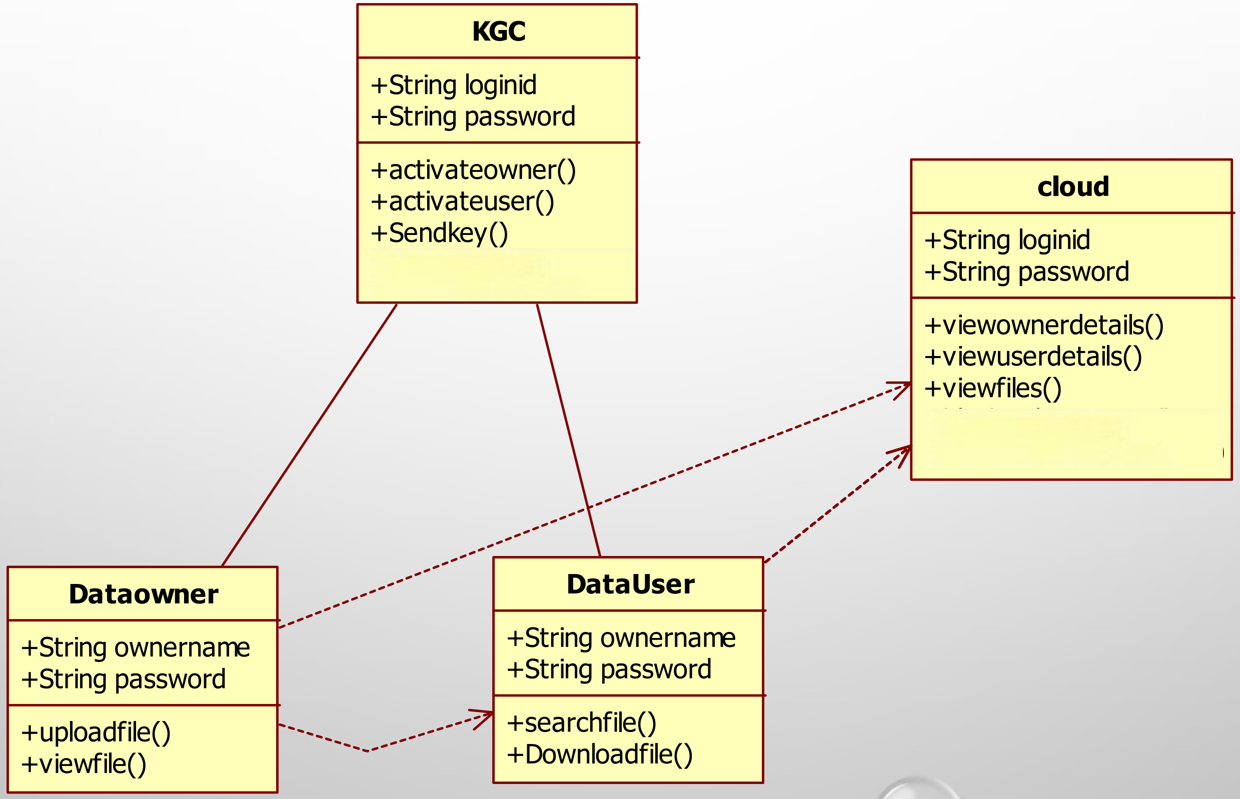
UML Diagrams

1. Use Case Diagrams
2. Class Diagrams
3. Sequence Diagrams
4. Activity Diagrams

Use Case Diagrams



Class Diagrams



KGC

+String loginid
+String password

+activateowner()
+activateuser()
+Sendkey()

cloud

+String loginid
+String password

+viewownerdetails()
+viewuserdetails()
+viewfiles()

Dataowner

+String ownername
+String password

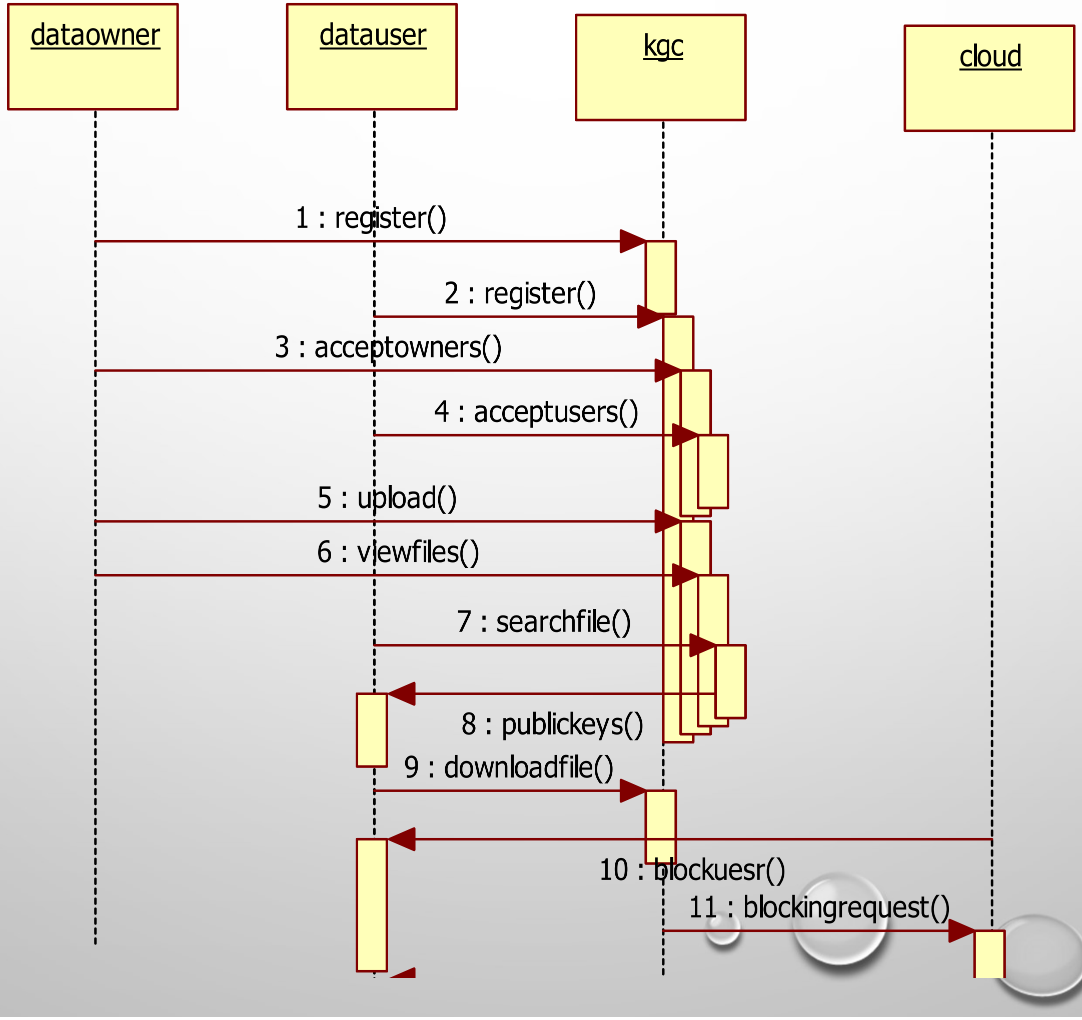
+uploadfile()
+viewfile()

DataUser

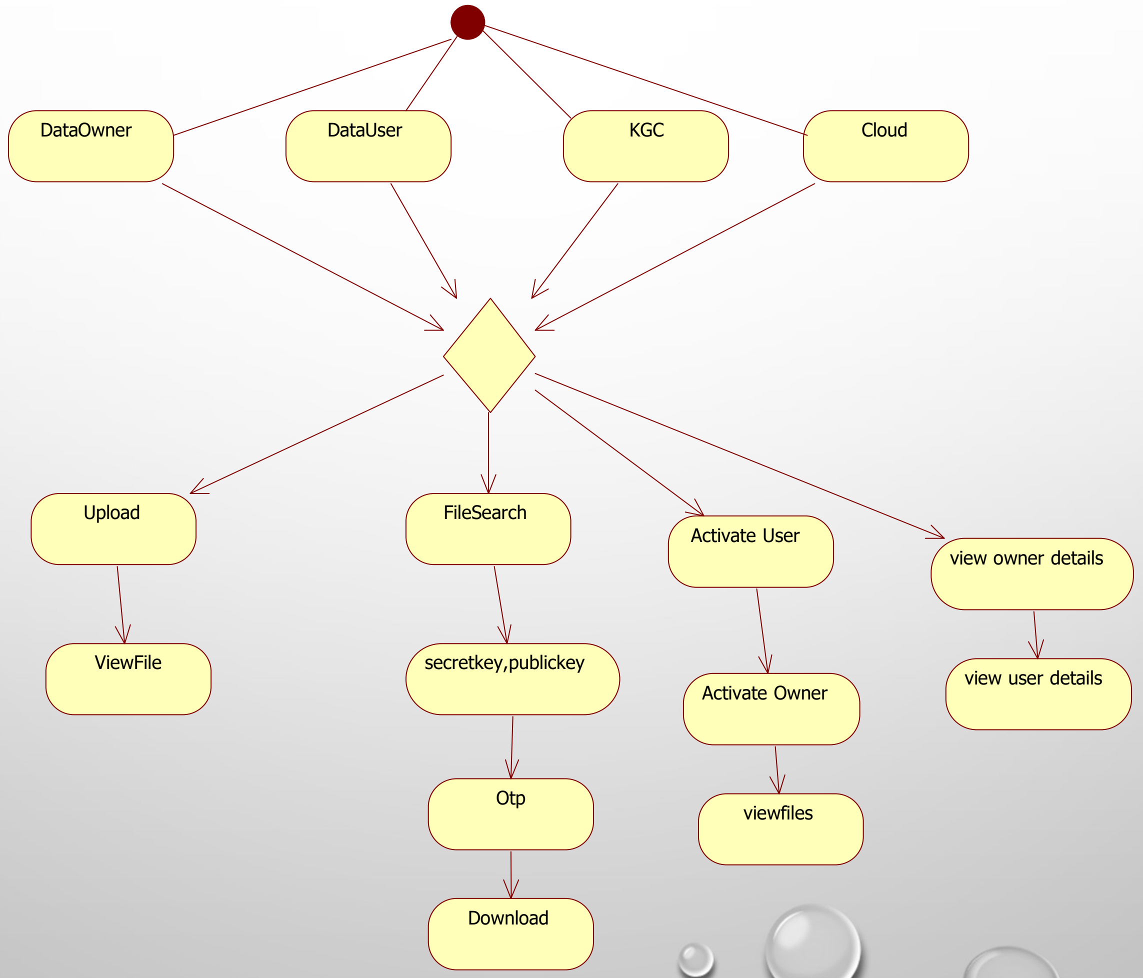
+String ownername
+String password

+searchfile()
+Downloadfile()

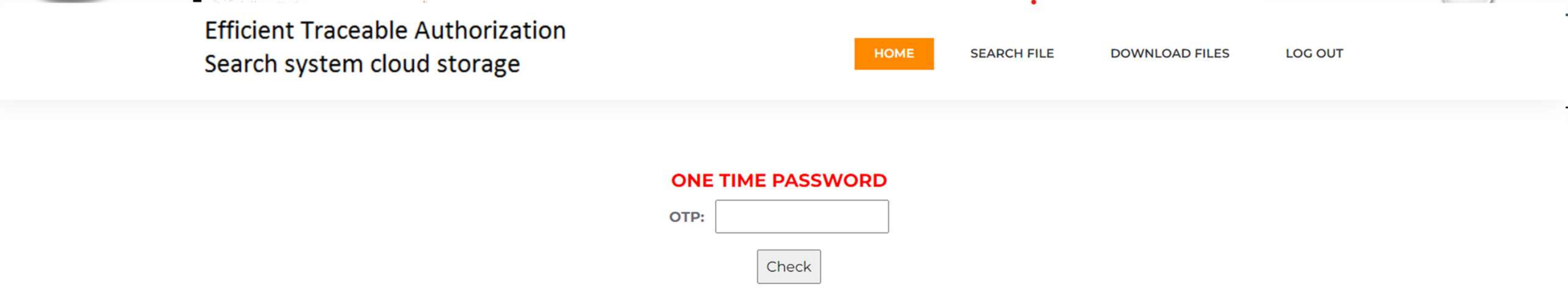
Sequence Diagrams



Activity Diagrams



Screenshots of Results

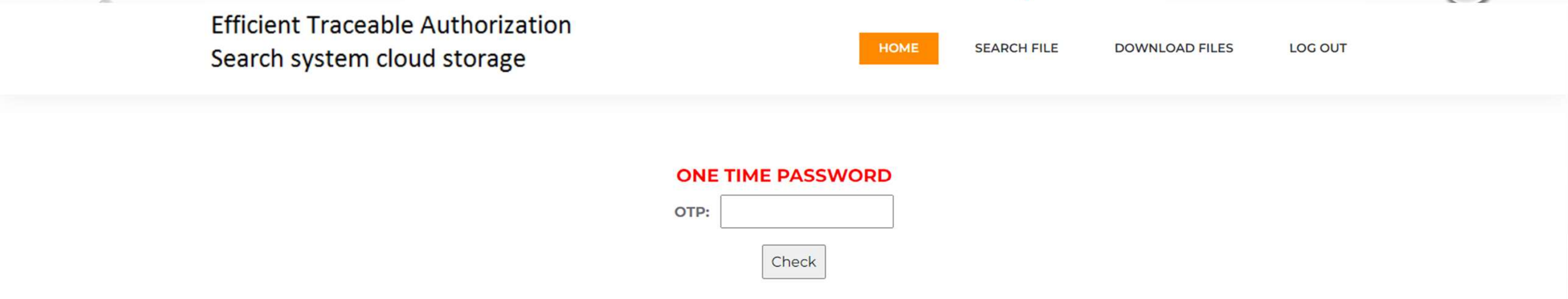


Efficient Traceable Authorization
Search system cloud storage

ONE TIME PASSWORD

OTP:

Test Cases



Efficient Traceable Authorization
Search system cloud storage

ONE TIME PASSWORD

OTP:

Conclusion

The enforcement of access control and the support of keyword search are important issues in secure cloud storage system. So in our project, we defined a new paradigm of searchable encryption system, and proposed a concrete construction.

The process involves the registration of both users and data owners, and the matching of their attributes or keywords to ensure that they are linked correctly. Once registered, both users and data owners need to be accepted by the KGC (Key Generation Center) and provided with public and private keys to access the cloud server.

Users can then search for files uploaded by the data owner and request details from KGC, who will check their authenticity and provide file details if verified. To access the file, KGC generates an OTP (One Time Password) that the user must enter correctly before being allowed to download the requested file from the cloud server. This process helps ensure the security and integrity of the data stored on the cloud server and restricts access to authorized users only.

References

- C. Wang, N. Cao, J. Li, K. Ren, W. Lou. "Secure ranked keyword search over encrypted cloud data"[c]//IEEE 30th international conference on distributed computing systems (ICDCS), IEEE, 2010: 253-262.
- Q. Zhang, L. T. Yang, Z. Chen, P. Li, M. J. Deen. “Privacy-preserving double-projection deep computation model with crowd sourcing on cloud for big data feature learning,” IEEE internet of things journal, 2017, DOI: 10.1109/jiot.2017.2732735.
- R. Chen, Y. Mu, G. Yang, F. Guo and X. Wang, “dual-server public- key encryption with keyword search for secure cloud storage,” IEEE transactions on information forensics and security, 2016, vol.11, no. 4, 789-798.
- R. Liu, R.H. Deng, K.K.R. Choo, J. Weng. ”An efficient privacy preserving outsourced calculation toolkit with multiple keys.” IEEE transactions on information forensics and security 11.11 (2016): 2401-2414.

Web Resources

- HTTPS://JPINFOTECH.ORG/EFFICIENT-TRACEABLE-AUTHORIZATION-SEARCH-SYSTEM-FOR-SECURECLOUD-STORAGE/
- HTTP://IEEEXPLORE.IEEE.ORG/DOCUMENT/8327889/
- HTTP://INPRESSCO.COM/SECURE-AND-EFFICIENT-TRACEABLE-AUTHORIZATION-MULTI-KEYWORDSEARCH-SYSTEM-FOR-CLOUD-STORAGE-USING-BLOCKCHAIN-TECHNOLOGY/

Thank You