International conference on Advanced Techniques in Communication Networking and Automation

RESEARCH ARTICLE OPEN ACCESS

Crypt Cloud+: Secure and Expressive Data Access Control for Cloud Storage

S.Jagatha[1],Dr.S.Arun[2] ,Dr.K.Kalaivani[3], 4.Mrs.K.Ulagapriya[4]

1.M.E CSE First Year,VISTAS,Chennai Email: vstm2016@gmail.com

2.Dr.S.Arun-CSE,VISTAS,Chennai,Email: arun.se@velsuniv.ac.in

3.Dr.K.Kalaivani-CSE,VISTAS,Chennai,Email: kalai.se@velsuniv.ac.in

4. Mrs.K.Ulagapriya-CSE,VISTAS,Chennai,Email: Upriya.se@velsuniv.ac.in

Abstract

Data owners will store their data in public cloud along with encryption and particular set of attributes to access control on the cloud data. While uploading the data into public cloud they will assign some attribute set to their data. If any authorized cloud user wants to download their data they should enter that particular attribute set to perform further actions on data owner's data. A cloud user wants to register their details under cloud organization to access the data owner's data. Users want to submit their details as attributes along with their designation. Based on the user details Semi-Trusted Authority generates decryption keys to get control on owner's data. An user can perform a lot of operations over the cloud data. If the user wants to read the cloud data he needs to be entering some read related attributes, and if he wants to write the data he needs to be entering write related attributes. Foe each and every action user in an organization would be verified with their unique attribute set. These attributes would be shared by the admins to the authorized users in cloud organization. These attributes will be stored in the policy files in a cloud. If any user leaks their unique decryption key to the any malicious user data owners wants to trace by sending audit request to auditor and auditor will process the data owners request and concludes that who is the guilty.

OBJECTIVE OF THE PROPOSED SYSTEM:

The main aim of this project is to provide integrity of an organization data which is inpublic cloud.

INTRODUCTION

The prevalence of cloud computing may indirectly incur vulnerability to the confidentiality of outsourced data and the privacy of cloud users. A particular challenge here is on how to guarantee that only authorized users can gain access to the data, which has been outsourced to cloud, at anywhere and anytime. One naive solution is to employ encryption technique on the data prior to uploading to cloud. However, the solution limits further data sharing and processing. This is so because a data owner needs to download the encrypted data from cloud and further re-encrypt them for sharing (suppose the data owner has no local copies of the data). A fine-grained access control over encrypted data is desirable in the context of cloud computing.

Cipher text Policy Attribute-Based Encryption (CPABE) may be an effective solution to guarantee the confidentiality of data and provide fine-grained access control here. In a CP-ABE based cloud storage system, for example, organizations (e.g., a university such as the University of Texas at San Antonio) and individuals (e.g., students, faculty members and visiting scholars of the university) can first specify access policy over attributes of a potential cloud user. Authorized cloud users then are granted access credentials (i.e., decryption keys) corresponding to their attribute sets (e.g., student role, faculty member role, or visitor role), which can be used to obtain access to the outsourced data. As a robust one-to-many encryption mechanism, CP-ABE offers a reliable method to protect data stored in cloud, but also enables fine-grained access

Control over the data.

SYSTEM ANALYSIS

EXISTING SYSTEM:

In existing system the CP-ABE may help us prevent security breach from outside attackers. But when an insider of the organization is suspected to commit the "crimes" related to the redistribution of decryption rights and the circulation of user information in plain format for illicit financial gains, how could we conclusively determine that the insider is guilty? Is it also possible for us to revoke the compromised access privileges? In addition to the above questions, we have one more which is related to key generation authority. A cloud user's access credential (i.e., decryption key) is usually issued by a semi-trusted authority based on the attributes the user possesses. How could we guarantee that this particular authority will not (re-)distribute the generated access credentials to others.

DISADVANTAGE:

- To preserve cloud data confidentiality and user privacy, cloud data are often stored in an encrypted form. But duplicated data that are encrypted under different encryption schemes uld be stored in the cloud, which greatly decreases the utilization rate of storage resources, especially for big data.
- Expressive, Efficient and Revocable Data Access Control for Multi-Authority Cloud Storage
- Cloud storage does trigger some newsecurity threats to data owners.

PROPOSED SYSTEM:

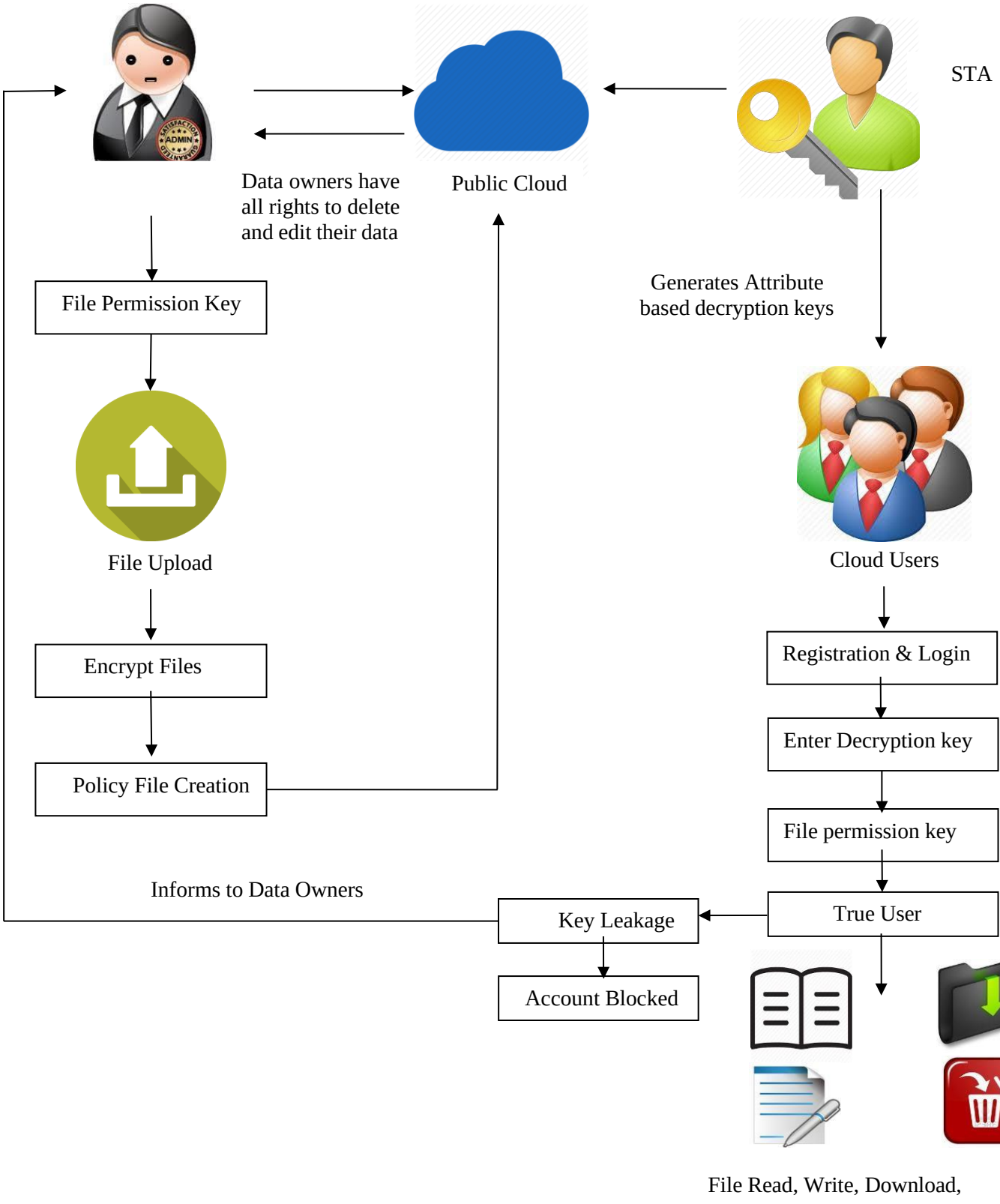
In this work, we have addressed the challenge of credential leakage in CP-ABE based cloud storage system by designing an accountable authority and revocable Crypt Cloud which supports white-box traceability and auditing (referred to as Crypt Cloud+). This is the first CP-ABE based cloud storage system

that simultaneously supports white-box traceability, accountable authority, auditing and effective revocation. Specifically, Crypt Cloud+ allows us to trace and revoke malicious cloud users (leaking credentials). Our approach can be also used in the case where the users' credentials are redistributed by the semi-trusted authority.

ADVANTAGES:

- It provably secure against chosen cipher-text attacks.
- We can easily foresee that these securityconcerns and requirements would become more urgent in the coming era of cloud computing wherein individuals,organizations, and businesses may outsource their various types of data, include ing the highly sensitive data, into the cloud.
- Reducing cloud users' burden of storage management and equipmentmaintenance.
- Avoiding investing a large amount of hardware and software.
- Enabling the data access independent

Proposed system Architecture:



Modules:

- Organization profile creation & Key Generation
- Data Owners File Upload
- File Permission & Policy File Creation
- Tracing who is guilty

Modules description:

Organization profile creation & Key Generation

User has an initial level Registration Process at the web end. The users provide their own personal information for this process. The server in turn stores the information in its database. Now the Accountable STA (semi-trusted Authority) generates decryption keys to the users based on their Attributes Set (e.g. name, mail-id, contact number etc..,). User gets the provenance to access the Organization data after getting decryption keys from Accountable STA.

Data Owners File Upload

In this module data owners create their accounts under the public cloud and upload their data into public cloud. While uploading the files into public cloud data owners will encrypt their data using RSA Encryption algorithm and generates public key and secret key. And also generates one unique file access permission key for the users under the organization to access their data.

File Permission & Policy File Creation

Different data owners will generate different file permission keys to their files and issues those keys to users under the organization to access their files. And also generates policy files to their data that who can access their data. Policy File will split the key for read the file, write the file, download the file and delete the file.

Tracing who is guilty

Authorized DUs are able to access (e.g. read, write, download, delete and decrypt) the outsourced data. Here file permission keys are issued to the employees in the organization based on their experience and position. Senior Employees have all the permission to access the files (read, write, delete, & download). Fresher's only having the permission to read the files. Some Employees have the permission to read and write. And some employees have all the permissions except delete the data. If any Senior Employee leaks or shares their secret permission keys to their junior employees they will request to download or delete the Data Owners Data. While entering the key system will generate attribute set for their role in background validate that the user has all rights to access the data. If the attributes set is not matched to the Data Owners policy files they will be claimed as guilty. If we ask them we will find who leaked they key to the junior employees.

Hardware Environment

The hardware requirements may serve as the basis for a contract for the implementation of the system and should therefore be a complete and consistent specification of the whole system. They are used by software engineers as the starting point for the system design. It shows what the systems do and not how it should be implemented.

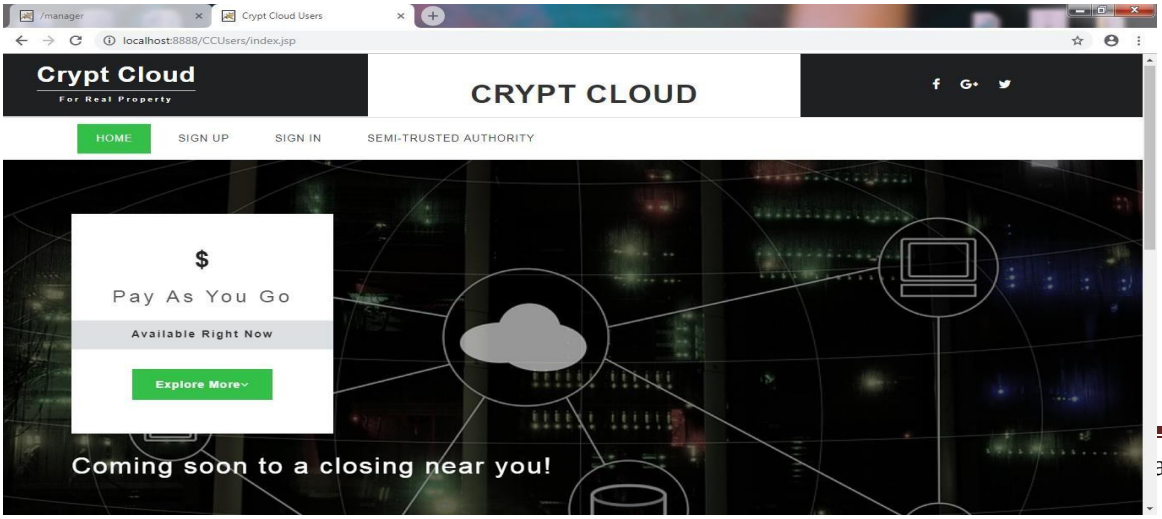
- Hard Disk : 80GB and Above
- RAM : 4GB and Above
- Processor : P IV and Above

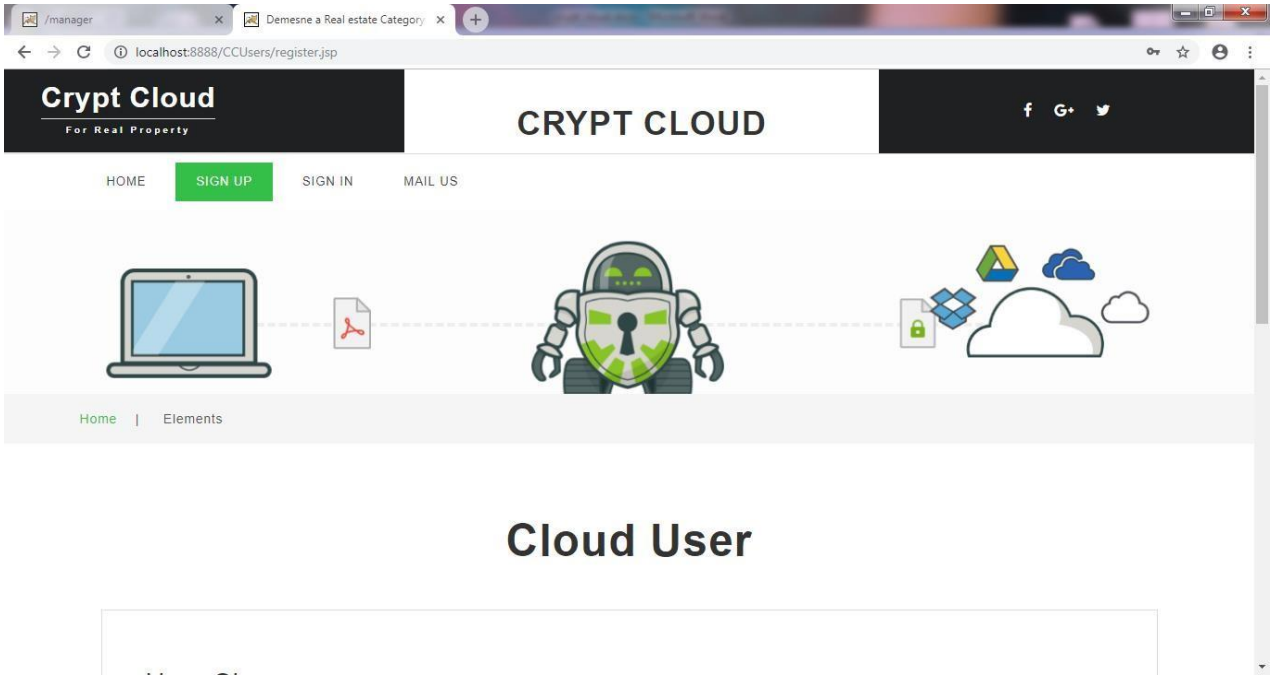
Software Environment

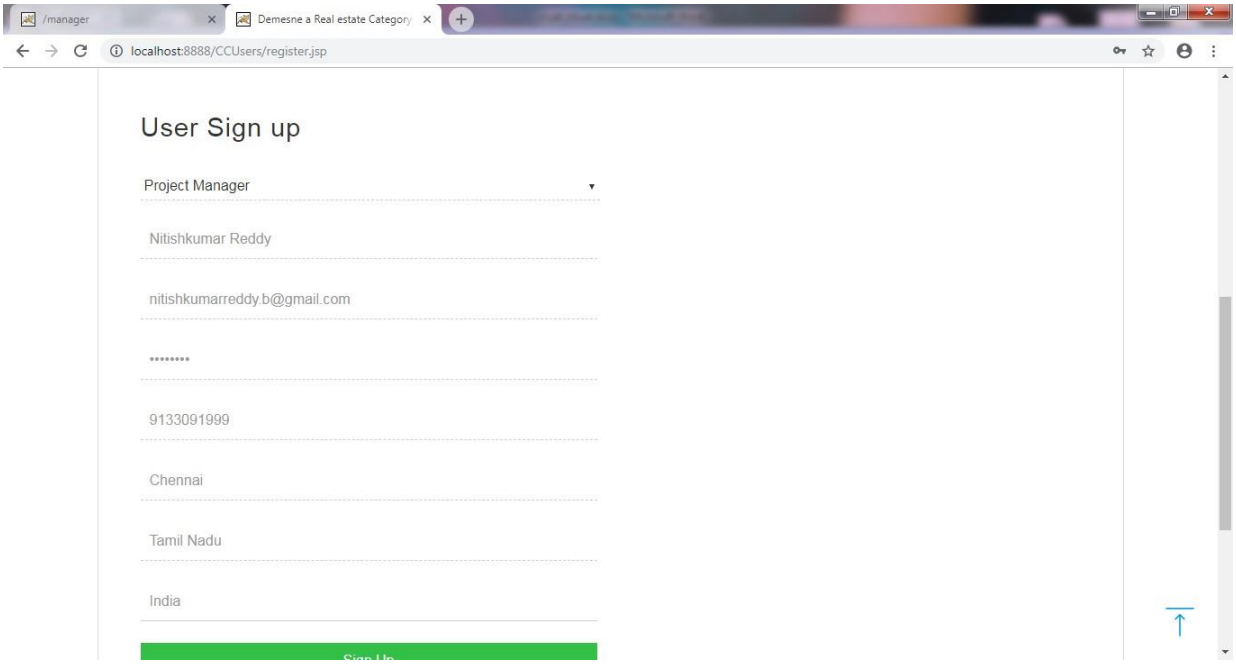
The software requirements are the specification of the system. It should include both a definition and a specification of requirements. It is a set of what the system should do rather than how it should do it. The software requirements provide a basis for creating the software requirements specification.

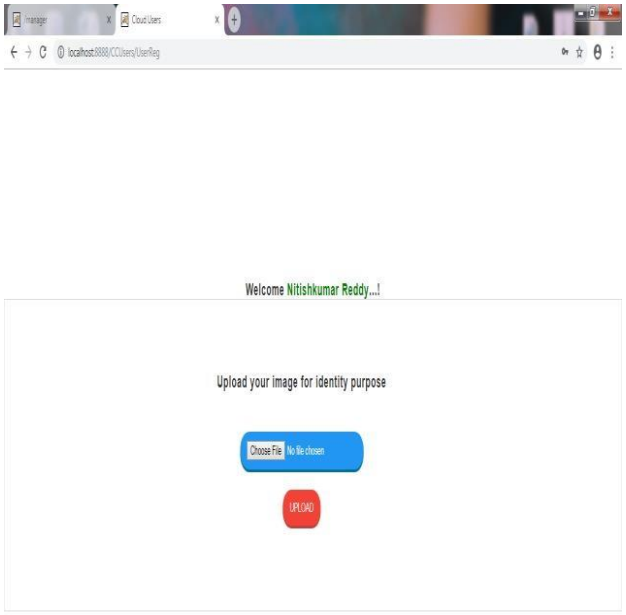
- Windows 7 and above
- JDK 1.7
- J2EE
- Tomcat 7.0
- MySQL

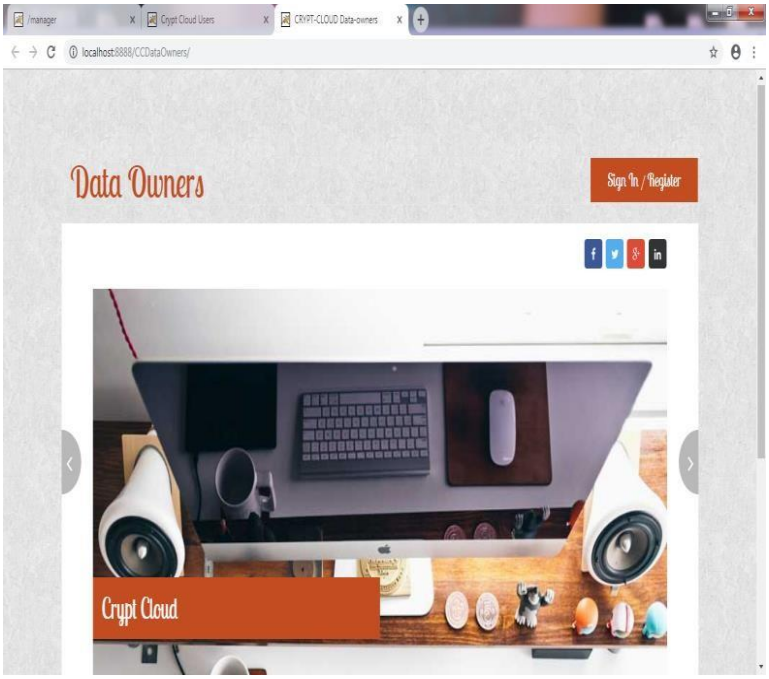
Screenshot:

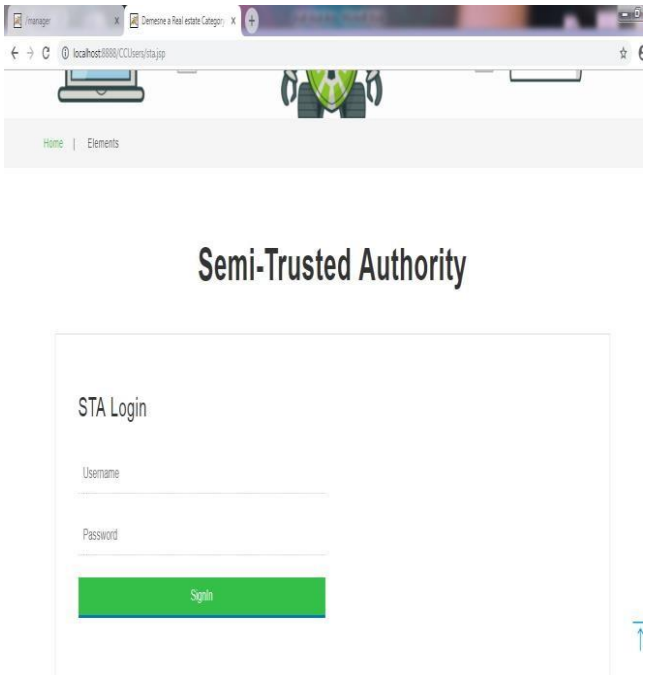


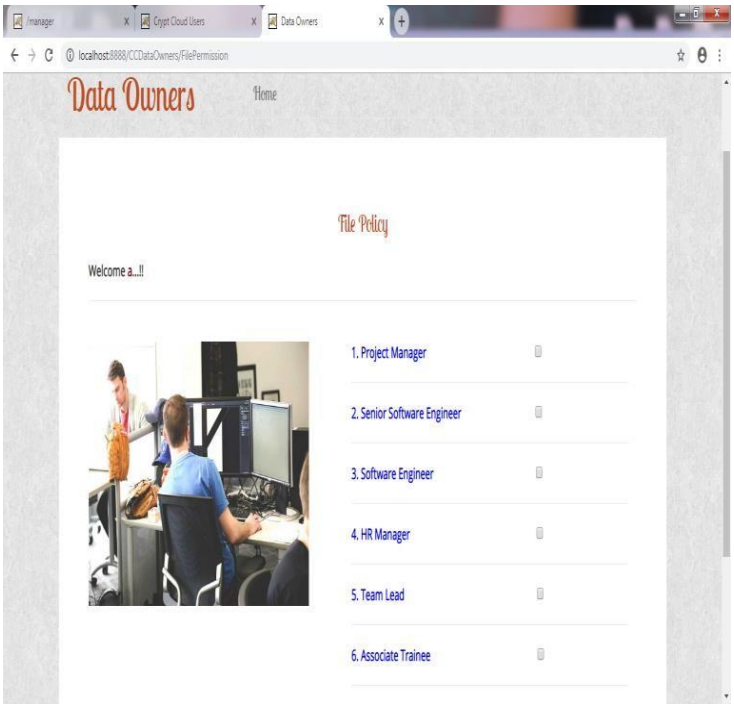

/manager
Demesne a Real estate Category
localhost:8888/CCUsers/register.jsp
Crypt Cloud
For Real Property
CRYPT CLOUD
HOME
SIGN UP
SIGN IN
MAIL US
Home | Elements
Cloud User

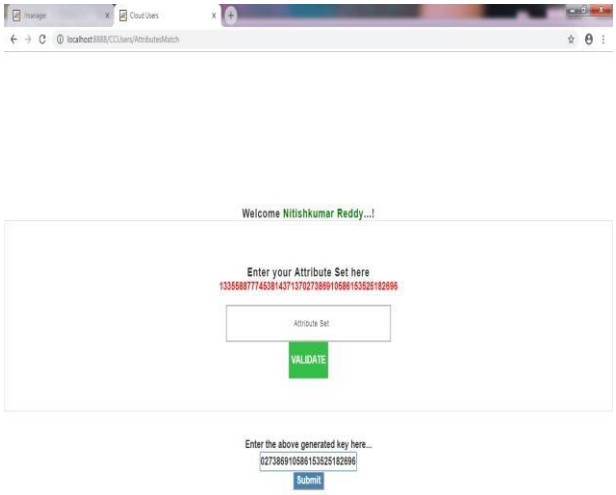

/manager
Demesne a Real estate Category
localhost:8888/CCUsers/register.jsp
User Sign up
Project Manager
Nitishkumar Reddy
nitishkumarreddy.b@gmail.com
9133091999
Chennai
Tamil Nadu
India

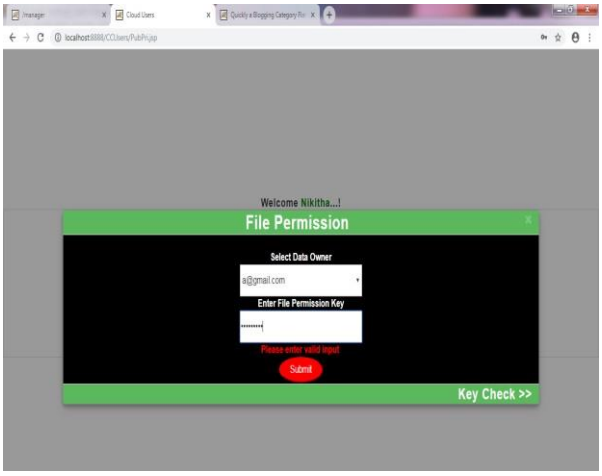

Welcome Nitishkumar Reddy...!
Upload your image for identity purpose
Choose File
No file chosen
UPLOAD

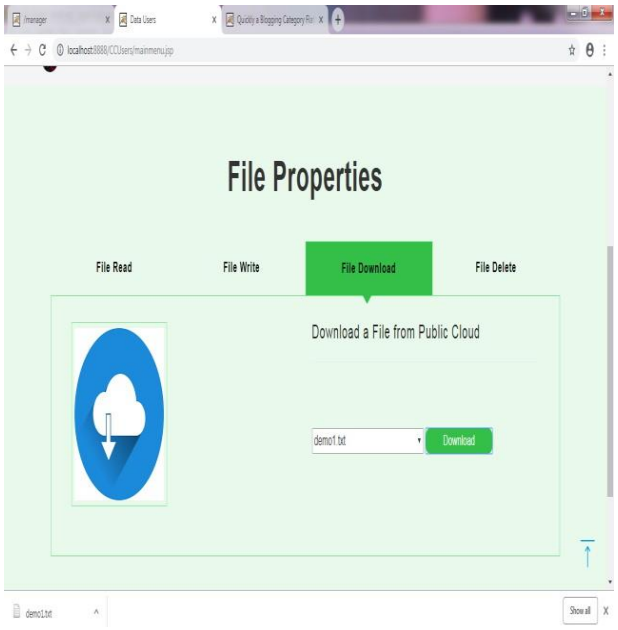

Data Owners
Sign In / Register
Crypt Cloud

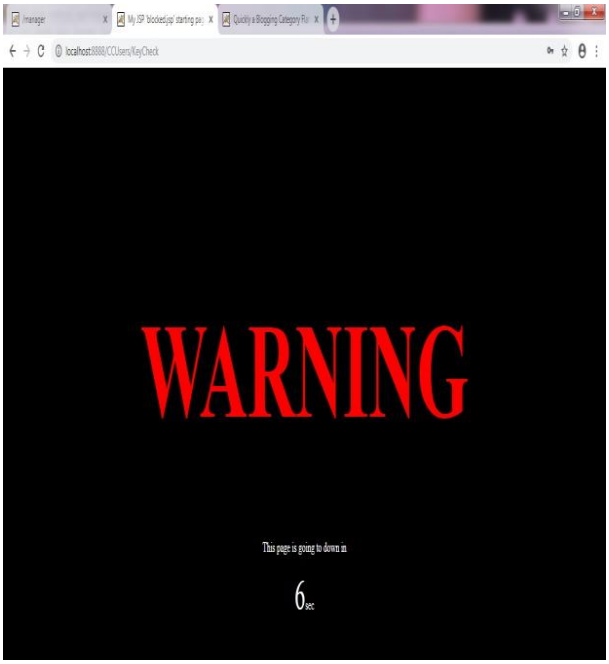

Home | Elements
Semi-Trusted Authority
STA Login
Username
Password
SignIn


Data Owners
Home
File Policy
Welcome a...!!
1. Project Manager
2. Senior Software Engineer
3. Software Engineer
4. HR Manager
5. Team Lead
6. Associate Trainee


Welcome Nitishkumar Reddy...!
Enter your Attribute Set here
Attribute Set
VALIDATE
Enter the above generated key here...
Submit


Welcome Nikitha...!
File Permission
Select Data Owner
Enter File Permission Key
Please enter valid input
Submit
Key Check >>


File Properties
File Read
File Write
File Download
File Delete
Download a File from Public Cloud
demo1.txt
Download


WARNING
This page is going to down in
6 sec

Conclusion

In this work, we have addressed the challenge of credential leakage in CP-ABE based cloud storage system by designing an accountable authority and revocable CryptCloud which supports white-box traceability and auditing (referred to as CryptCloud+). This is the first CP-ABE based cloud storage system that simultaneously supports white-box traceability, accountable authority, auditing and effective revocation. Specifically, CryptCloud+ allows us to trace and revoke malicious cloud users (leaking credentials). Our approach can be also used in the case where the users' credentials are redistributed by the semi-trusted authority. We note that we may need black-box traceability, which is a stronger notion (compared to white-box traceability), in CryptCloud. One of our future works is to consider the black-box traceability and auditing

REFERENCES

1. Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li, and Albert Y. Zomaya. Sedasc: Secure data sharing in clouds. IEEE Systems Journal, 11(2):395–404, 2017.
2. Mazhar Ali, Samee U. Khan, and Athanasios V. Vasilakos. Security in cloud computing: Opportunities and challenges. Inf. Sci., 305:357–383, 2015.
3. Michael Armbrust, Armando Fox, R ean Griffith, Anthony D Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, et al. A view of cloud computing. Communications of the ACM, 53(4):50–58, 2010.
4. Nuttapong Attrapadung and Hideki Imai. Attribute-based encryption supporting direct/indirect revocation modes. In Cryptography and Coding, pages 278–300. Springer, 2009.
5. Amos Beimel. Secure schemes for secret sharingand key distribution. PhD

thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

6. Mihir Bellare and Oded Goldreich. On defining proofs of knowledge. In Advances in Cryptology-CRYPTO'92, pages 390–420. Springer, 1993.
7. Dan Boneh and Xavier Boyen. Short signatures without random oracles. In EUROCRYPT - 2004, pages 56–73, 2004.
8. Hongming Cai, Boyi Xu, Lihong Jiang, and Athanasios V. Vasilakos. Iot-based big data storage systems in cloud computing: Perspectives and challenges. IEEE Internet of Things Journal, 4(1):75–87, 2017.
9. Jie Chen, Romain Gay, and Hoeteck Wee. Improved dual system ABE in prime-order groups via predicate encodings. In Advances in Cryptology - EUROCRYPT 2015, pages 595–624, 2015.
10. Angelo De Caro and Vincenzo Iovino. jpbc: Java pairing based cryptography. In ISCC 2011, pages 850–855. IEEE, 2011.
11. Hua Deng, Qianhong Wu, Bo Qin, Jian Mao, Xiao Liu, Lei Zhang, and Wenchang Shi. Who is touching my cloud. In Computer Security-ESORICS 2014, pages 362–379. Springer, 2014.
12. Zhangjie Fu, Fengxiao Huang, Xingming Sun, Athanasios Vasilakos, and Ching-Nung Yang. Enabling semantic search based on conceptual graphs over encrypted outsourced data. IEEE Transactions on Services Computing, 2016.
13. Vipul Goyal. Reducing trust in the PKG in identity based cryptosystems. In Advances in Cryptology-CRYPTO 2007, pages 430–447. Springer, 2007.
14. Vipul Goyal, Steve Lu, Amit Sahai, and Brent Waters. Black-box accountable authority identity-based encryption. In Proceedings of the 15th ACM conference on Computer and communications security, pages 427–436. ACM, 2008.
15. Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine- grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer and communications security, pages 89–98. ACM, 2006.