INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE

ISSN: 2057-5688

CRYPTOGRAPHICALLY ENFORCED DYNAMIC ACCESS CONTROL IN THE CLOUD TECHNOLOGY

BONDU SUNIL KUMAR [1], UDAYALAKSHMI [2]

[1]Assistant professor, [2] Assistant Professor

CSE Department, Sri *Mittapalli College* of *Engineering*, *Guntur*, *Andhra Pradesh*-522233

Abstract- Enabling cryptographically enforced access controls for data hosted in untrusted cloud is attractive for many users and organizations. However, designing efficient cryptographically enforced dynamic access control system in the cloud is still challenging. In this paper, we propose Crypt-DAC, a system that provides practical cryptographic enforcement of dynamic access control. Crypt-DAC revokes access permissions by delegating the cloud to update encrypted data. In Crypt-DAC, a file is encrypted by a symmetric key list which records a file key and a sequence of revocation keys. In each revocation, a dedicated administrator uploads a new revocation key to the cloud and requests it to encrypt the file with a new layer of encryption and update the encrypted key list accordingly. Crypt-DAC proposes three key techniques to constrain the size of key list and encryption layers. As a result, Crypt-DAC enforces dynamic access control that provides efficiency, as it does not require expensive decryption/reencryption and uploading/re-uploading of large data at the administrator side, and security, as it immediately revokes access permissions. We use formalization framework and system implementation to demonstrate the security and efficiency of our construction.

I. INTRODUCTION

Crypt-DAC A file is encrypted by a symmetric key list which records a file key and sequence of revocation key. In each revocation, a dedicated administrator uploads a new revocation key to the cloud and requests it to encrypt the file with a new layer of encryption and update the encrypted key list accordingly.

II. LITERATURE SURVEY

A. Existing System

- Garrison et al. proposed two revocation schemes. The first scheme requires an administrator to re-encrypt file with new keys as discussed above. Instead, the second scheme delegates users to re-encrypt the file when they need to modify the file, relieving the administrator from re-encrypting file data by itself.
- Wang et al. proposed another revocation scheme, in which the symmetric homomorphic encryption scheme is used to encrypt the file. Such a design enables the cloud to directly re-encrypt file without decryption.

DISADVANTAGES OF EXISTING SYSTEM:

- This scheme incurs a considerable communication overhead.
- This scheme, however, comes with a security penalty as the revocation operation is delayed to the next user's modification to the file. As a result, a newly revoked user can still access the file before the next writing operation.
- This scheme incurs expensive file read/write overhead as the encryption/decryption operation involves comparable overhead with the public key encryption schemes: paging delegation delegates and audits the kernel's paging operations to a secure space; execution trapping intercepts the (compromised) kernel's attempts to subvert SecPod by misusing privileged instructions. We have implemented a prototype of SecPod based on KVM. Our experiments show that SecPod is both effective and efficient.

B. PROPOSED SYSTEM:

- We present Crypt-DAC, a cryptographically enforced dynamic access control system on untrusted cloud. Crypt-DAC delegates the cloud to update encrypted files in permission revocations. In Crypt-DAC, a file is encrypted by a symmetric key list which records a file key and a sequence of revocation keys. In a revocation, the administrator uploads a new revocation key to the cloud, which encrypts the file with a new layer of encryption and updates the encrypted key list accordingly
- First, Crypt-DAC proposes delegation-aware encryption strategy to delegate the cloud to update policy data.

ISSN: 2057-5688

- Second, Crypt-DAC proposes adjustable onion encryption strategy to delegate the cloud to update file data.

ADVANTAGES OF PROPOSED SYSTEM:

- Crypt-DAC achieves efficient revocation, efficient file access and immediate revocation simultaneously.
- For revocation efficiency, Crypt-DAC incurs lightweight communication overhead at the administrator side as it does not need to download and reupload file data.
- For immediate revocation, the permissions of users are immediately revoked as the files are re-encrypted. For file access efficiency, the files are still encrypted by symmetric keys
- Crypt-DAC periodically removes the bounded encryption layers of files while amortizing the burden to a large number of writing users.

III. METHODOLOGY

A. ADJUSTABLE ONION ENCRYPTION:

Adjustable onion encryption enables the administrator to delegate the cloud provider to update Files. The administrator only needs to upload a new revocation key to the cloud provider. Upon receiving the key, the cloud provider uses it to encrypt the files with a new layer of encryption and then deletes it. To constrain the size of the encryption layers, adjustable onion encryption provides two modes: security mode and efficiency mode. Such a design enables the administrator to define a tolerable bound for a file. Initially, the strategy works in the security mode and the encryption layers increase as revocations happen. Once the size of the encryption layers reaches the bound, it turns to the efficiency mode to constrain the encryption layers by putting more trust on the cloud. As a result, the administrator can flexibly adjust a tolerable bound for each file according to file type, access pattern, etc., to achieve a balance between efficiency and security

B. KEY ROTATION SCHEME:

Key rotation is a scheme which a sequence of keys can be produced from an initial key and a secret key. Only the owner of the secret key can derive the next key in the sequence, but any user knowing a key in the sequence can derive all previous versions of the key.

C. ACCESS CONTROL ADMINISTRATOR:

The access control administrator is responsible for managing access policies of the file data. It assigns/revokes access permissions by creating, updating, and distributing cryptographic keys used to encrypt files.

D. USERS:

Users may download any policy/file data from the cloud, but are only allowed to decrypt and read files according to their access permissions.

E. CLOUD PROVIDER:

The cloud provider is responsible for the data storage and management. The data includes file data of users in the company, as well as policy data regulating access policies for these files. Both the policy/file data are encrypted prior to being uploaded to the cloud provider.

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

IV. RESULT

A. Home Page:

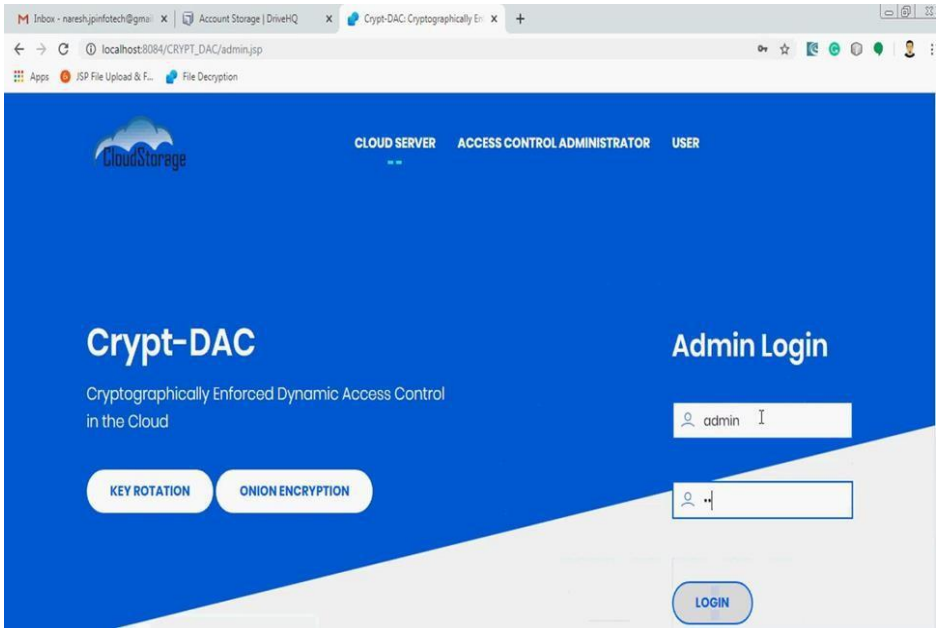


Fig 1: Home Page.

B. User Registration page

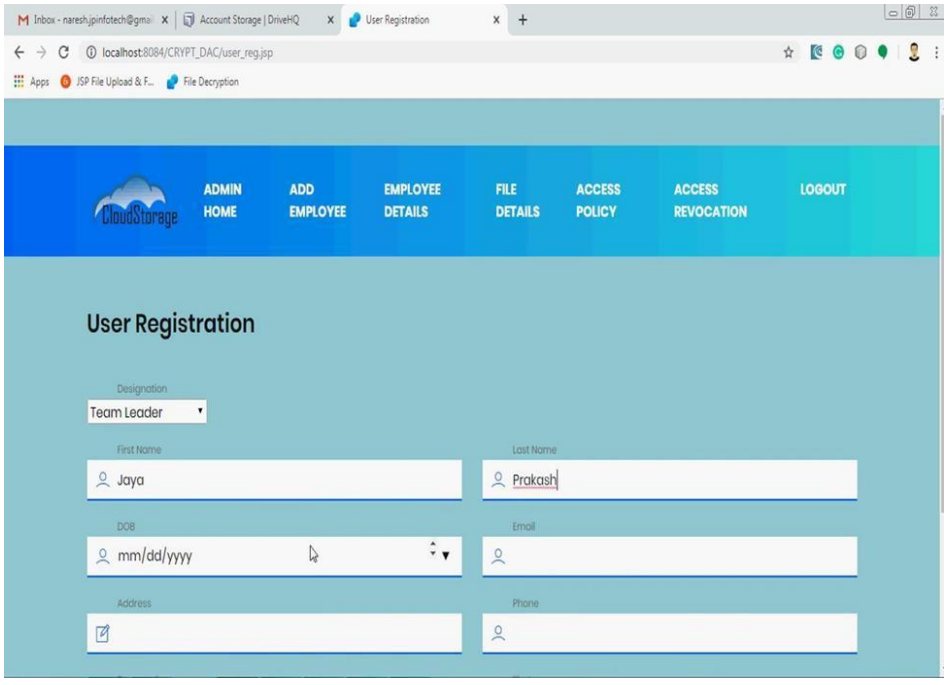


Fig 2: Setting Page.

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

C. Regestration confirmation mail

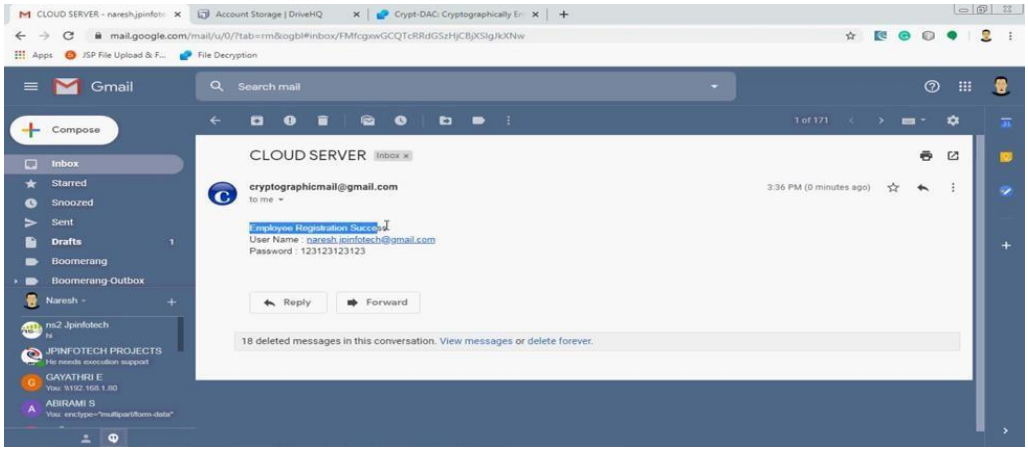
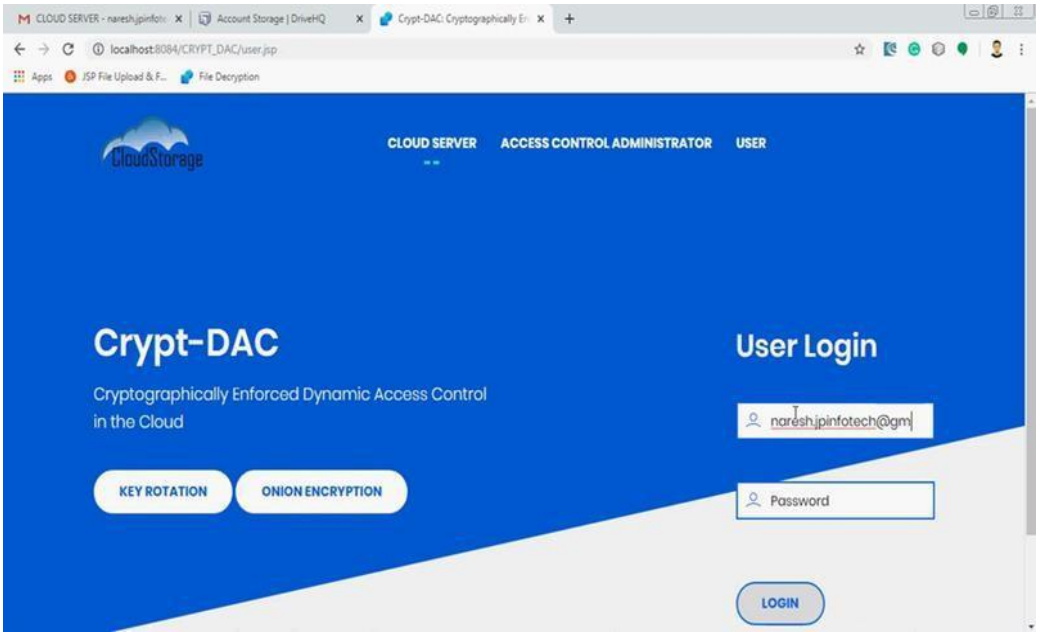
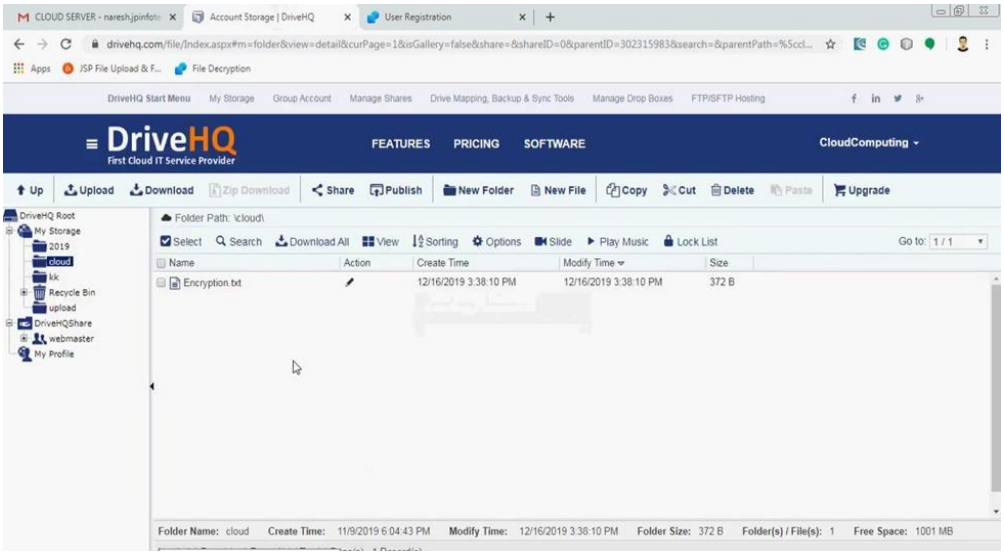


Fig 3: Regestration Confirmation page

D. Login Page

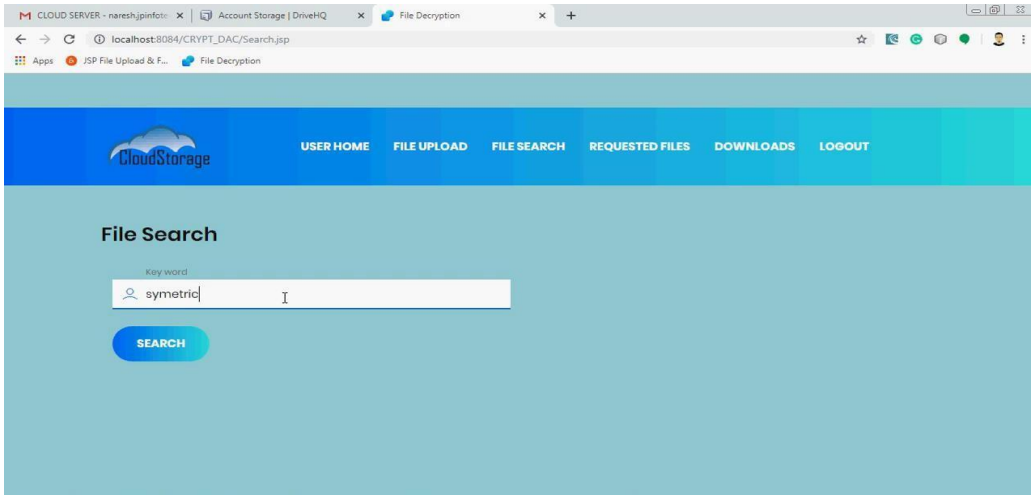


E. Cloud

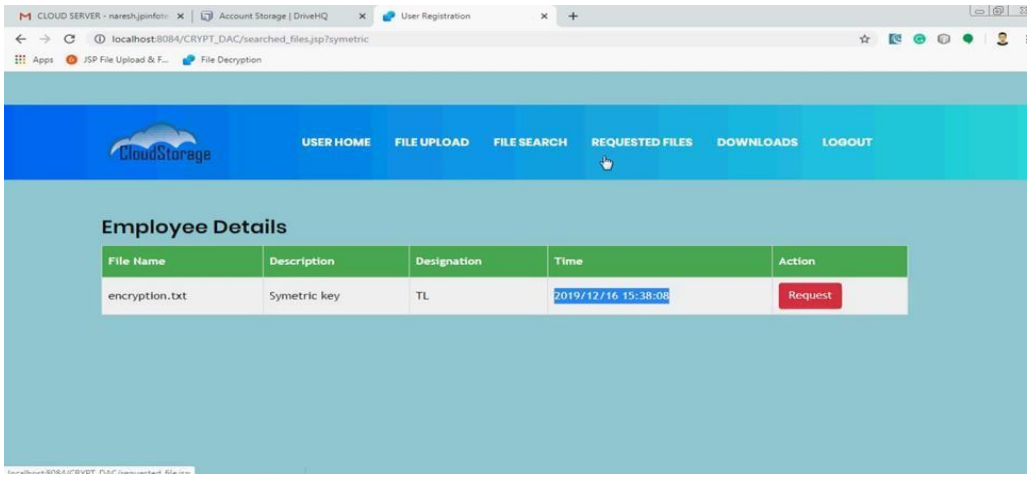


INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

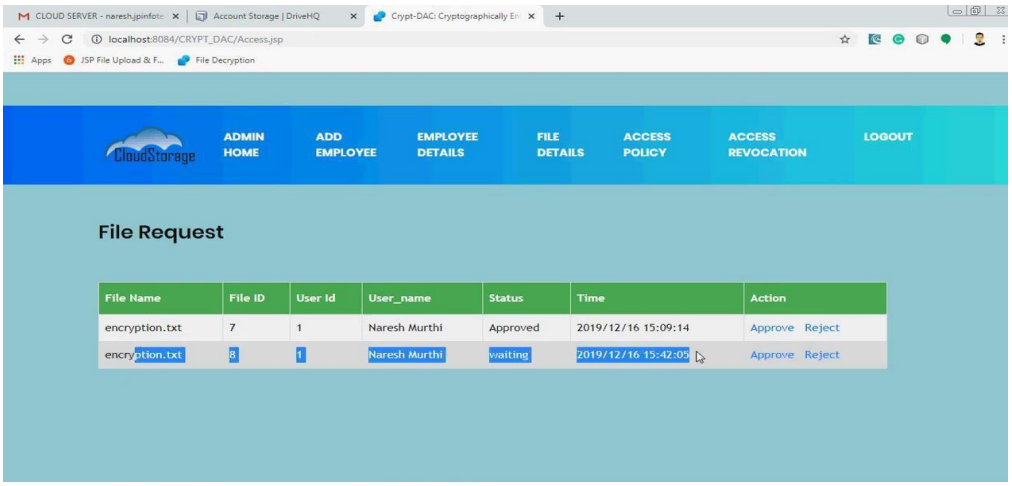
F Searching file



G. User Requesting file

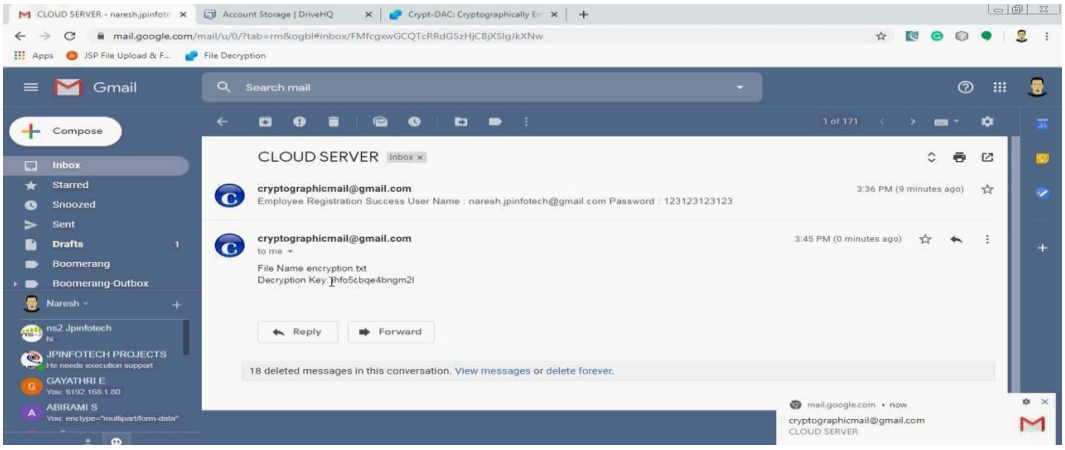


H. Admin page

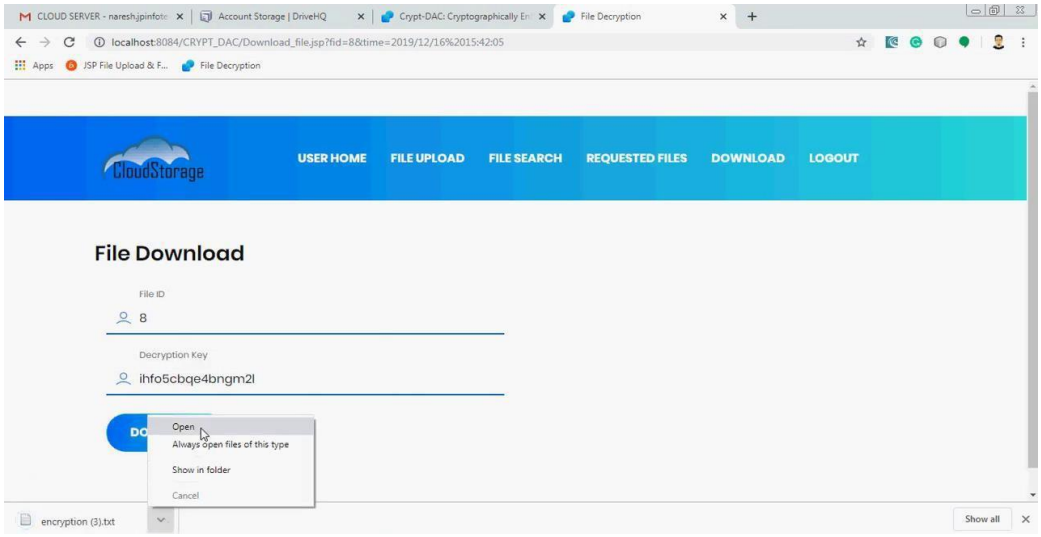


INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

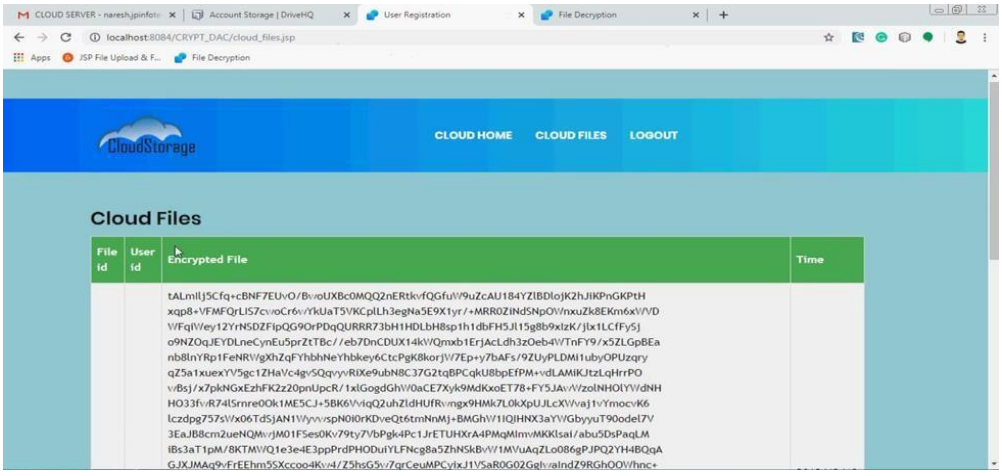
I. Decryption Key



J. User downloading file



K. Cloud Files



V. CONCLUSION

We presented Crypt-DAC, a system that provides practical cryptographic enforcement of dynamic access control in the potentially untrusted cloud provider. Crypt-DAC meets its goals using three techniques. In particular, we propose to delegate the cloud to update the policy data in a privacy-preserving manner using a delegation-aware encryption strategy. We propose to avoid the expensive re-encryptions of file data at the administrator side using a adjustable onion encryption strategy. In addition, we propose a delayed de-onion

ISSN: 2057-5688

encryption strategy to avoid the file reading overhead. The theoretical analysis and the performance evaluation show that Crypt-DAC achieves orders of magnitude higher efficiency in access revocations while ensuring the same security properties under the honest but- curious threat model compared with previous schemes.

VI. REFERENCES

[1] "Road Accidents in India 2018". Available: https://morth.nic.in/sites/default/files/Road_Accidednt.pdf, pp. 1-125

[2] Forsman, Pia M., et al. "Efficient driver drowsiness detection at moderate levels of drowsiness." Accident Analysis & Prevent ion 50 (2013): 341-350.

[3] Simon, Michael, et al. "EEG alpha spindle measures as indicators of driver fat igue under real traffic condit ions." Clinical Neurophysiology 122.6 (2011): 1168-1178.

[4] Massoz, Quent in, et al. "The ULg multimodality drowsiness database (called DROZY) and examples of use." 2016 IEEE Winter Conference on Applications of Computer Vision (WACV). IEEE, 2016.

[5] Svensson, U. Blink behavior based drowsiness detection. No. LiUIMT- EX-04/369,. 2004.

[6] Bergasa, Luis Miguel, et al. "Real-time system for monitoring driver vigilance." IEEE Transact ions on Intelligent Transportation Systems 7.1 (2006): 63-77.

[7] Zhihong, Wu, and Xiao Xiaohong. "Study on histogram equalization." Intelligence Information Processing and Trusted Comput ing, International Symposium on. IEEE Computer Society, 2011.

[8] Kubinger, Wilfried, Markus Vincze, and Minu Ayromlou. "The role of gamma correction in colour image processing." 9th European Signal Processing Conference (EUSIPCO 1998). IEEE, 1998.

[9] Kazemi, Vahid, and Josephine Sullivan. "One millisecond face alignment with an ensemble of regression trees." Proceedings of the IEEE conference on computer vision and pat tern recognition. 2014.

[10] Dalal, Navneet, and Bill Triggs. "Histograms of oriented gradients for human detect ion." 2005 IEEE computer society conference on computer vision and pat tern recognit ion (CVPR'05). Vol. 1. IEEE, 2005.