International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 3 No: 4 June 2018

Securing Cloud Data under Key Exposure

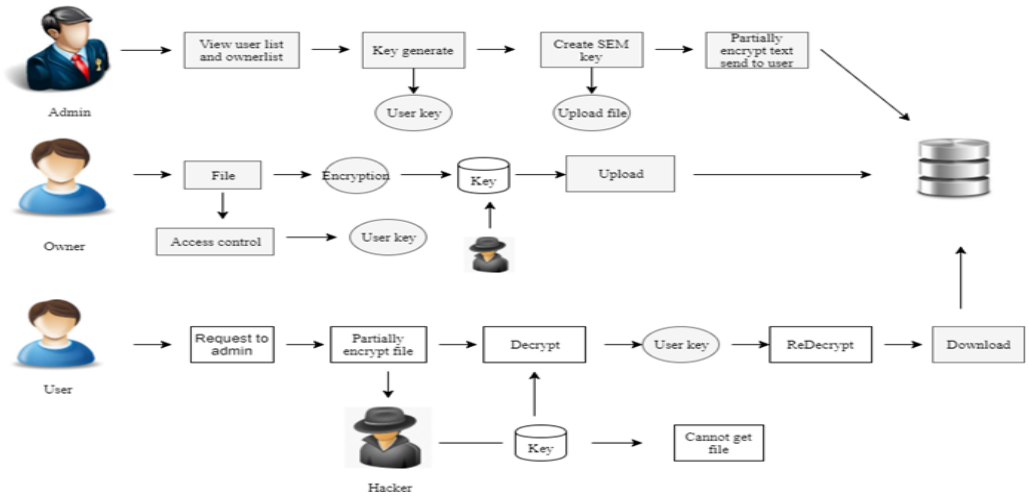
Azham Hussain
School of Computing, Universiti Utara Malysia, Kedah, Malaysia

Abstract: The world recently witnessed a massive surveillance program aimed at breaking users privacy. Recent news reveal a powerful attacker which breaks data confidentiality by acquiring cryptographic keys, by means of coercion or back doors in cryptographic software. Once the encryption key is exposed, the only viable measure to preserve data confidentiality is to limit the attacker's access to the ciphertext. ciphertext blocks across servers in multiple administrative domains thus assuming that the adversary cannot compromise all of them the world recently witnessed a massive surveillance program aimed at breaking users privacy. If the user upload the some file in the cloud while encrypting the data, but the hackers , whose know the key they hack that file very easily, so we provide a bastion algorithm, Bastion first encrypts the data with one round of block cipher encryption, and then applies an efficient linear post-processing to the ciphertext By doing so, Bastion relaxes the notion of all-or-nothing encryption at the benefit of increased performance ,so in this way we secure the owner files, if the file encrypted buy the owner, and then the owner give the authority to the user whose only download the file. In user side the all owner upload files are viewed, but if the user give the request to the authority file only ,otherwise if the one user did not have the authority to download the file, first the user give the request to the cloud service provider, the owner give the authority to the file is partially encrypted and send to the user, if the owner did not give the authority to the user , the file is not viewed, the data owner did not share this file to you message is displayed, but by mistake the cloud service provider accept the user request, that file send to that user but the user did not download the file.

1. PROPOSED SYSTEM

In proposed, the owner upload the encrypted file in the cloud, and then they give the download authority to the particular user in the cloud, so if the authority user only download that file, but if the (hacker) non authority user download to give the request to the cloud service provider, the admin verify the user request only they download the file, after the admin verify the partial key is send to the user. Then the authorized user, Re-encrypt that file and download. And in the file is not viewed to the unauthorized user. so they did not download and also the file is not viewed.

2. ARCHITECTURE DIAGRAM



International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 3 No: 4 June 2018

Advantage

- Hacker did not hack the file
- Re-encryption
- Security.

Module Explanation:

Upload: The owner upload the file, in upload time the owner give the access control to the particular user, so that user only can download the file and then encrypt the file. And also the owner update the access control .The other user for example, the access cannot give user cannot download the file.

Access Control: The access control means the owner give the access to the users , the access control key is user key, so the owner set access to user and then only encrypt the file, In download time the user want the file, the first Decrypt the file, after once again Redecrypt the file with user key.

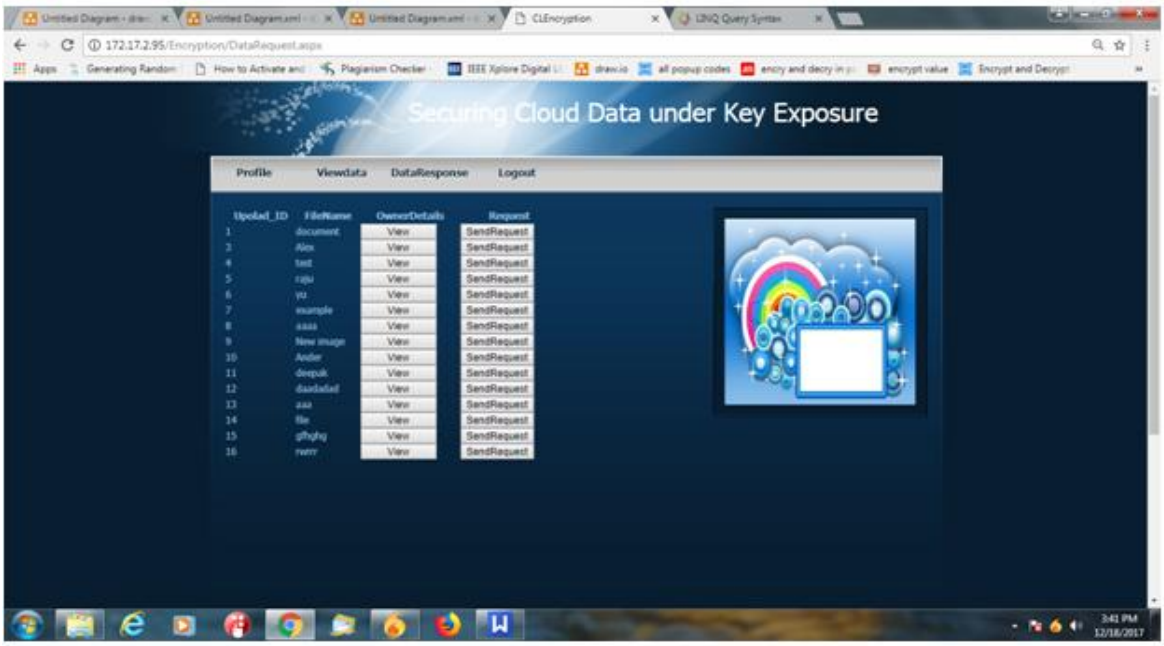
Data Response: The all files in the cloud are viewed by the user, if the user view the owner details and then give the request to the admin for the download the file. The cloud service provider verify the user request, after that if the owner give the authority to the user the partially encrypt file is displayed and then that file is send to the user, otherwise, the owner did not give access control to the user , the data owner did not share this file message is displayed. And then the user decrypt the file using the user key.

Download: In download time, the cloud service provider accept the user request and then send the file, first the decrypt the file and then the user re decrypt the file using the user key, so the owner gave authority to the user only can download the file, other user cannot download the file because the authority given user have the use key so that user only download the file.

Key Generation Center: The admin generate the key for the user, if the user is registered, so the user key is the password for the user, and then in upload time the owner give authority to the that user key, while using the user key the other users like hackers cannot hack the owner file, if the hacker hack the encrypt key but the hacker do not have the user key so they did not get the file.

Sem Key: The SEM key means split key encryption management, the cloud service provider use this key only secured the upload files. the key is generate for the upload files, if the user give the request to the user that time the admin send the SEM key to the that user use this key the file partially encrypt and then send to the user, the hacker also get the partially encrypt file, and then the user use the user key for download the file.

Implementation



3. CONCLUSION

In the conclusion, The files in the cloud are very secured the did no t hack the owner file in the cloud because the cloud service provider a high secure to the upload files while in the download time also the cloud service provider create the two key for the user one is the user key and another one is the SEM key(Split Key Encryption).So in this way the hackers cannot hack the upload file in the cloud.

REFERENCES

[1] Rivest R.L(1997) All-or-nothing encryption and the package transform.in Biham E.(eds) fast software Encryption. FSE 1997.lecture Notes in computer science,vol 1267,spring,Berlin,Heidelberg.

[2] conditionally secure secret sharing schemes with disenrollment capability Chris Charnes, Josef pieprzyk, rei safavi-naini department of computer science university of Wollongong.

[3] Mohammad Reza Zakerinasab,Mea Wang,"practical Network Coding for the Update Problem in Cloud Storage System",Network and Service Management IEEE Transactions on,vol,14,pp,386-400,2017,ISSN 1932-4537.

[4] Xiangyu Luo,Yun Wang,Zhuowei Shen,"On the impact of erasure coding parameters to the reliability of distributed brick storage system"Cyber-Enabled Distributed Computing and knowledge Discovery 2009 CyberC '09 International Conference on pp 250-256,2009.

[5] Efficient Dispersal of Information for Security Load Balancing,and Fault Tolerance Michael O. Rabin Harvard University, Cambridge, Massachusetts.

[6] Robust data sharing with key-value stores,cristina basescu, Christian cachin,Robert Haas,vrije universite it Amsterdam, Amsterdam, The Netherland.

