**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**
**IMPACT FACTOR: 5.258**

***IJCSMC, Vol. 5, Issue. 4, April 2016, pg.410 – 415***

# Enhancing Own Cloud Privacy Using Client Side Encryption

**Megha P[1], Devaki P[2]**
[1]Student, M.Tech-CNE, NIE & VTU, Mysore-Karnataka, India
[2]Associate Professor, Information and Science, NIE, Mysore-Karnataka, India
[1] meghap88@gmail.com; [2] p_devaki1@yahoo.com

***Abstract— As Smartphone users are increasing, with mobile applications are growing rapidly. Smartphone users expect personal computer like functionalities, smart phone is easily carried out and provides much computer functionality, such as processing, communication, data storage as well as many computers services such as web browser, video or audio player, video call, GPS, wireless network. But In Smartphone limited cpu processing, memory, batteries are limited. However, smart phone have to come long way in terms of security. to Enhance the smartphone feature, usually cloud are integrate with the mobile application. Not only just integrating with own cloud with that client side encryption will enhance the privacy of user data so Encryption is used for security of information in data storage and transmission process.***

***Keywords— Own Cloud, Drop Box, Encryption, Android, Files***

## I. INTRODUCTION

Smart phones are much similar to utilising as personal computers but few equipment restrictions, batteries, processing force are constrained, therefore, numerous application designers are compelled to take into record these restrictions. To unravel this asset issue, some looks into have proposed utilizing server assets in the cloud for Smartphone's and gadgets are supplanting tablets and customary PCs. These gadgets are utilized for correspondence as well as for mixed media applications, for example, listening to music, watching recordings, and playing diversions. Consequently the storage room accessible on these gadgets restricts the amount of interactive media documents can be utilized on the gadget and the client is continually expelling documents to make space to include new ones. Expansion of additional storage room either by expanding interior stockpiling by producers or expansion of SD cards just serves to briefly all the issue until us come up short on space once more. There is a need to for all time take care of this issue and coordination to cloud based capacity richly takes care of this issue. Cloud Based Record System takes care of this issue by giving at whatever time. With these encryption is included customer side to give more security to client information.

## II. ANDROID

Android Open Handset Alliance is an open source versatile working framework created by Google and the Open Handset Alliance. It is based on top of the Linux part and gives a SDK to application improvement in Java. Android utilizes the Dalvik Virtual Machine to execute applications. Dalvik is streamlined to keep running on gadgets with obliged CPU, memory, and force assets. It actualises a subset of Java 2 Platform Standard Edition (J2SE) utilising libraries from the Apache Harmony Apache Java execution, giving it preference over other ortable stages that just bolster Java 2 Platform Micro Release (J2ME), which is constrained by examination. Java class les must be aggregated to Dalvikbytecode (.dex position) and bundled in an .apk record with a specific end goal to be utilized on Android. Android gives an interface to framework gadgets and
Administrations through an arrangement of Java bundles, including android OS, android Hardware, Android Location and android media. This makes it simple to get to and work on mixed media information, sensor values, framework asset use information, what's more, area data. Not at all like some portable working
Frameworks, Android applications can utilize the record framework straightforwardly, making it conceivable to oversee documents as on a customary Unix framework. Android additionally gives a shell interface, however it needs a large number of the capacities of a run of the mill Linux.
Numerous creators depicted Android application improvement essentials, which incorporate setting up Android development environment on the machine, AndroidManifest.xml record, Activities, Intents, and XMLlayouts. Jackson (2011) traces "three noteworthy segments of an Android improvement environment: Java, Eclipse,

Android" and gives guidelines on the most proficient method to download and introduce vital records to build up this environment. Felker (2011) does not unequivocally express the segments but rather Or maybe brings up that Java JDK, Android SDK, Eclipse IDE, what's more, Android ADT should be introduced and arranged on a Machine [1]. The strides gave by these two creators are standard. They show up in numerous books composed on Android advancement and are additionally introduced on authority Android site ("Installing the SDK"). Ableson, King, and Sen (2011) present "four essential segments of Android applications": Activity, Service, Broadcast Receiver, and Content Provider. It is noticed that "a specific Android application won't not contain these components, but rather will have no less than one of these components" [2]. Since Activity "shows a UI (client interface) and reacts to framework and client started occasions", it is utilized every now and again for Android applications. These Exercises are proclaimed in AndroidManifest.xml record, which gives "the establishment for any Android application". Exercises show their perspectives through XML designs and "impart" with each other through Intents. Clear comprehension of these ideas and Java programming dialect is an essential to begin actualizing the advancement systems utilized as a part of Android applications.

## III. ENCRYPTION

The **Advanced Encryption Standard** or **AES** is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to **encrypt** sensitive data.

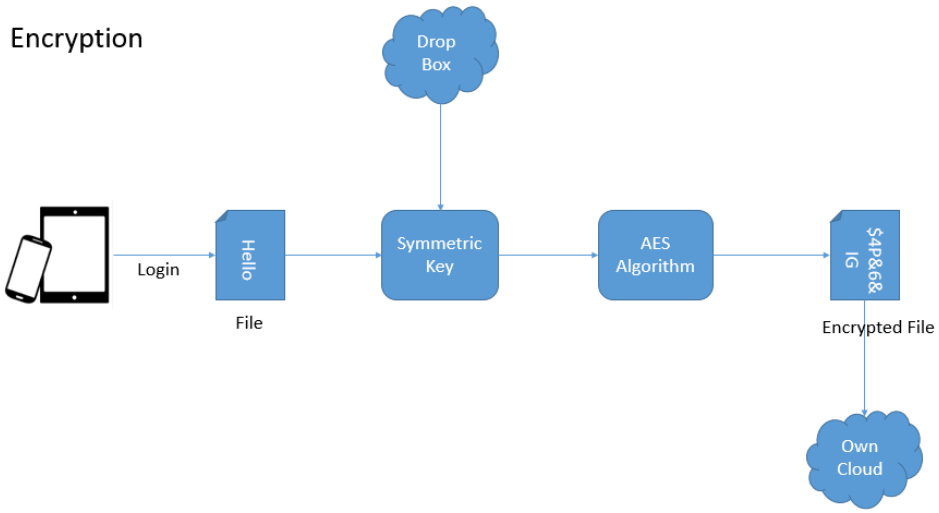



Fig.1 Encryption Architecture using DropBox & Own Cloud

Symmetric key cryptography is for the most part used to encode the information having vast sizes. Symmetric key algorithm is algorithm for cryptography that use the same cryptographic key for both encryption and decryption. The keys are identical but here we will store the key in Dropbox cloud and encrypted data will send to Own Cloud. By doing this, sending data will be more secure and even Admin not able to see the data. Above Fig 1 Proposed framework is performing in the encryption methodology: Fig1 demonstrates the encryption and unscrambling procedure of plaintext document. Encryption happens at sender side while unscrambling at recipient side. The information of encryption procedure is plaintext record and that of decoding procedure is the figure content document. In the first place plain content record is gone through the AES encryption calculation which encodes the plain content document using symmetric key and afterward deliver figure content record i.e. scrambled document is transmitted. Toward the end of unscrambling the info figure content document is gone through the AES decoding calculation which can unscramble the figure content document i.e. scrambled record utilizing the same key as that of encryption at last we get the first plain content document. The outcome appears the encryption and time.

## IV. OWN CLOUD

Own Cloud was begun is still kept up by Frank Karlitschek, the German open source programming designer. He exhibited at Camp KDE in 2010 [4]. Own Cloud gives protected, secure and agreeable document sync also, share arrangement on servers you control. It's open source record match up and share programming for everybody from people operation. With own cloud client can share one or more organizers on his/her PC, and sync them with own cloud server. Place records in client nearby shared catalogs, and those documents are quickly matched up to the server, and afterward to different PCs by means of the desktop customer. Basically sign in with the web customer and oversee private records there [5]. Below represent the principle structure of own cloud

1. Static IP Address
2. ReleaseKey: cd /tmp

wget http://download.opensuse.org/repositories/isv:ownCloud:community/xUbuntu_14.04/Release.key
sudo apt-key add - < Release.key

3. Repository: sudo sh -c "echo 'deb
http://download.opensuse.org/repositories/isv:/ownCloud:/community/xUbuntu_14.04/ /' >>
/etc/apt/sources.list.d/owncloud.list"
4. Database:

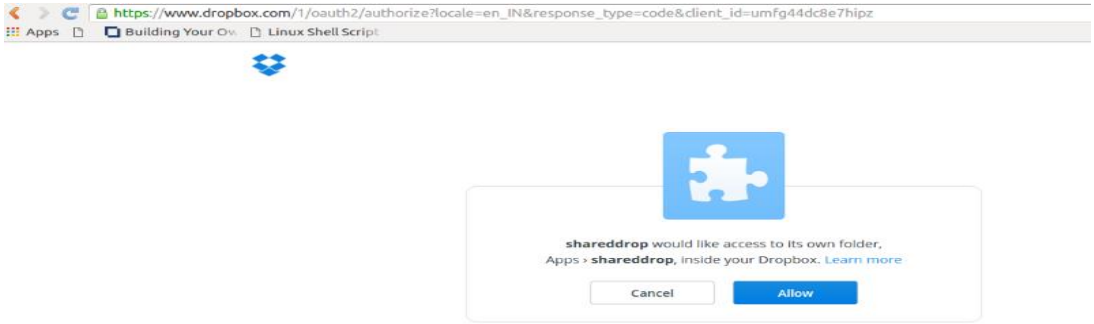
sudo sh -c "echo 'deb http://download.opensuse.org/repositories/isv:/ownCloud:/community/xUbuntu_14.04/
/' >> /etc/apt/sources.list.d/owncloud.list"

5. Configuration DB: sudo apt-get install mariadb-server
6. AdRepository:sudo sh -c "echo 'deb
http://download.opensuse.org/repositories/isv:/ownCloud:/community/xUbuntu_14.04/ /' >>
/etc/apt/sources.list.d/owncloud.list"

## V. RESULTS

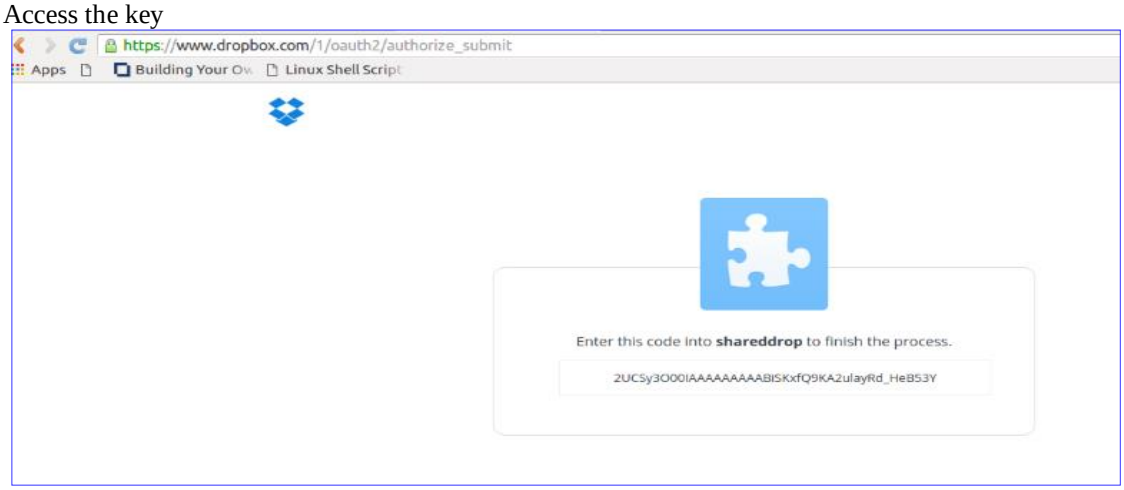
The below mentioned screen shots shows how the data is encrypting.

1. API Request Authorization DropBox

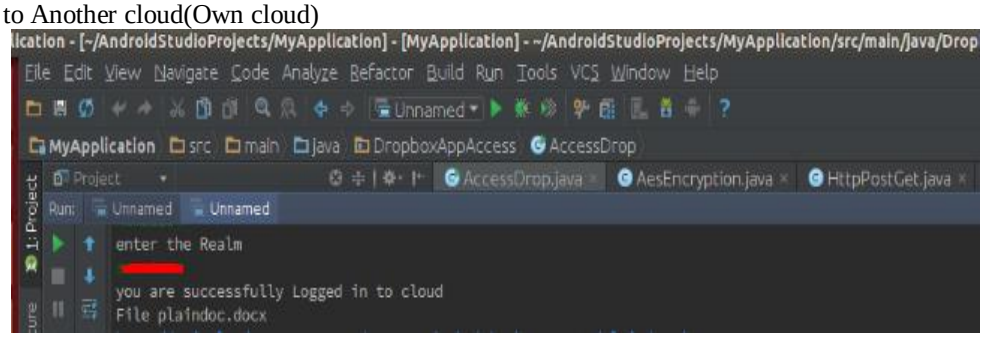


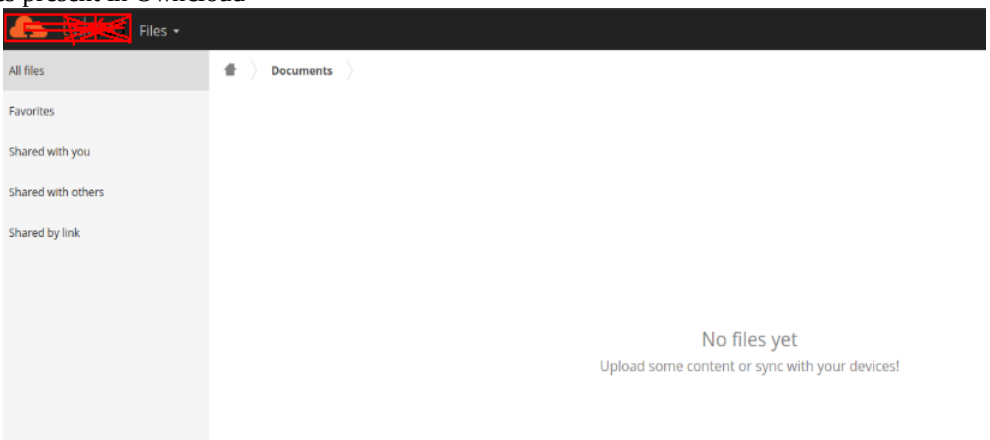
2. Access the key




3. Login to Another cloud(Own cloud)

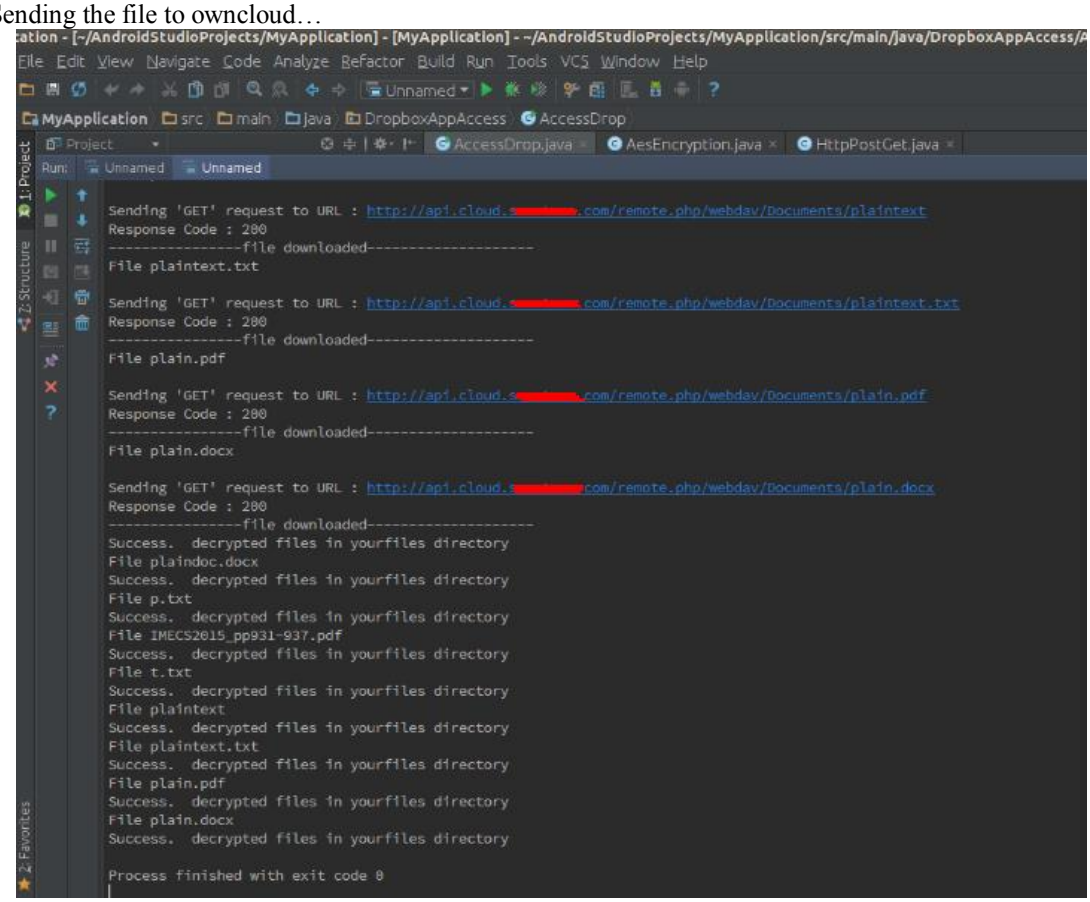



4. No files present in Owncloud

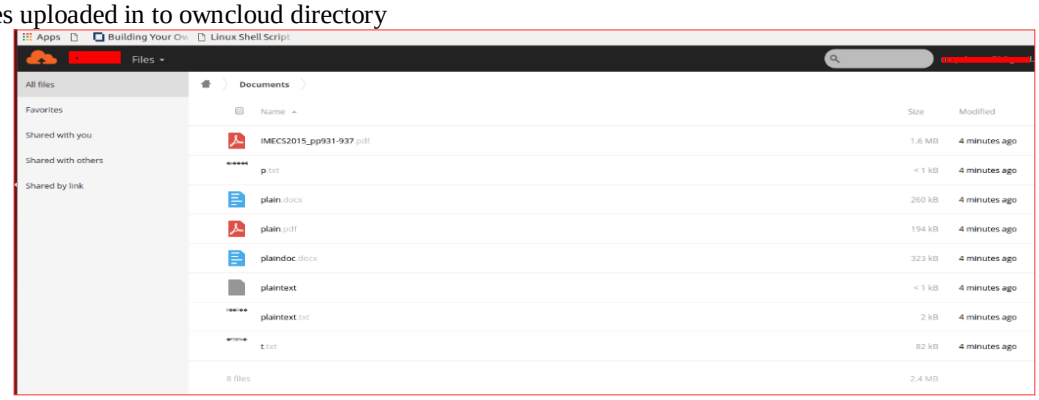


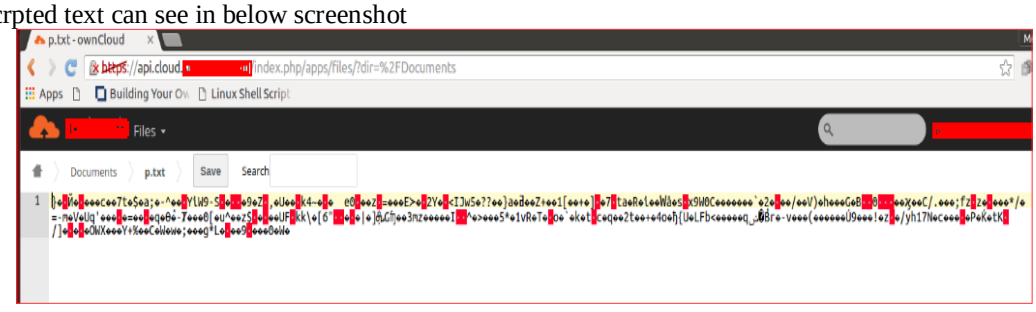
5. Sending the file to owncloud…




6. Files uploaded in to owncloud directory




7. Encrpted text can see in below screenshot



## VI. CONCLUSION

This paper shows successful implementation of files encryption. By doing this method, user feels more secure about his/her data. Even if he/she lost smart phone or if data corrupts then using dropbox cloud key, he can get back to previously uploaded files. Currently in market most of the competitors is using only one cloud service and if we lost mobile, it's very difficult to get back previously loaded files. Using 2 cloud services will be more secure.

## REFERENCES

[1] J. Breckling, Ed., *The Analysis of Directional Time Series: Applications to Wind Speed and Direction*, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.
[2] S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," *IEEE Electron Device Lett.*, vol. 20, pp. 569–571, Nov. 1999.
[3] J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.
[4] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11,1997.
[5] Bishop, T. (2011, March 6). "Google Play replaces Android Market, cosolidates Google's media commercial centers". Recovered from http://www.geekwire.com/2012/google-playreplaces-android-market-solidifies googles-media-commercial centers.
[6] Koziolek, H. (2011). "The sposad building style for multi-inhabitant programming applications". In Proc. 9 th Working IEEE/IFIP Conf. on Software Architecture (WICSA'11), Workshop on Architecting Cloud Computing Applications what's more, Systems, pages 320–327.IEEE.
[7] Http://en.wikipedia.org/wiki/OwnCloud.
[8] Https://owncloud.com.
[9] Http://doc.owncloud.org/server/6.0/ownCloudUserManual.
[10] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard.