Intuitive way of achieving secure data transfer and storage mechanism

Surbhi Gupta[*]

[*] Research and Development, Syscom Corporation Limited (A Morpho Company)

Abstract- Today, in this time where smart phones eco-system is well funded and thriving over PC or laptop eco-system. This is why majority of smart phone users tries to buy phone with maximum internal storage to store maximum possible data. Smart phones provide varying but limited size of internal storages on phones. To store data beyond the limit of internal storage, either you have to buy an SD card or by deleting old files to make room for new ones or upload the data on cloud storage with fear of loss of data.

There lies the prospect for an intuitive mode of memory sharing between two smart phones either in range or over a distance, connected through the internet. With this concept, we can solve the problem of extra large volumes of standalone storage space on a single device.

Index Terms- Internal Storage, Encryption, IOT, Cloud Server

I. Introduction

Being low on the internal storage on the phone causes so much of trouble. This lack of internal storage restricts your phone from installing application updates and in addition to store additional gigabytes of user data.

One of the solutions provided to this problem is expanded memory on phone through the addition of an external memory card. Though, this solution was considered as Kludge but somehow proven as a quick solution and effective to some extent. This concept of expanded memory worked till times when phone has support of this SD card. But today, Google has its phone in the market with no such support. The psychology behind not giving this support on phones is not limiting the internal storage but enhances the use of cloud services for backing-up and share the data. Cloud storage is not a mere tool to share data and forth from a device to the web but it could be an automated service having a check on what is shared when. Some of the examples of data storage over the cloud and Dropbox, Google Drive, Microsoft OneDrive, the files folders or other data which are shared with these virtual storage devices can automatically sync to each other's computer.

But we do aware about its conundrums which make the cloud data vulnerable to security breach:

a. Xml signature attacks using different types of signature wrapping.
b. Cross site scripting attacks where attackers can insert a piece of code into web applications, an example of this has already been seen with AMAZON being on the receiving end of the attack.
c. Denial of the service attack where malicious code is injected into the browser.

There are also many security issues from denial-of-service, law enforcement requests, and data stealing to flooding attack problems. In addition to this, surveys say that they lacked confidence in cloud provider's ability to properly handle data loss incidents.

There still needs a solution to keep your data safe in cases when users have no enough storage at their smart phones by using unused storage facility of other trusted smart device users. If the user is willing to share his/her storage space with friends and families and which will still be automated way and ensure the safe transfer and retrieval of user data.

II. Proposed Solution

The adequacy of information lies in the ways a problem is further categorized into. Suppose the problem of memory sharing becomes an obvious approach in the near future calculated over the probability of sharing becoming almost required by the common devices.

One obvious approach would be over the fast catching internet of things scenario (IOT), scenario where everything is connected to each other via a virtually wired connection. We can explain that with a beautifully flowing drawing, FIGURE 1.

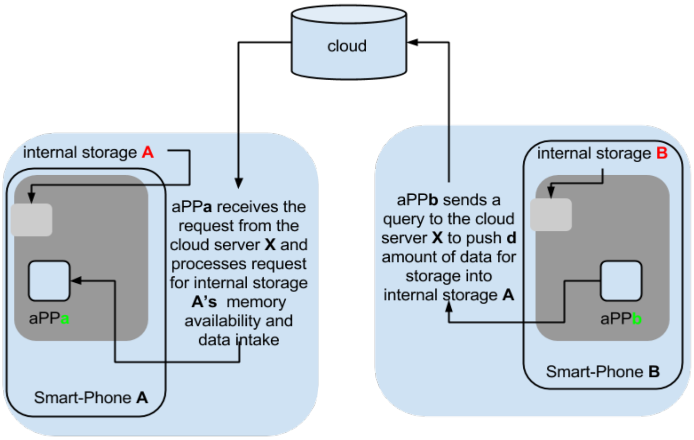
cloud
internal storage A
aPPa
Smart-Phone A
aPPa receives the request from the cloud server X and processes request for internal storage A's memory availability and data intake
aPPb sends a query to the cloud server X to push d amount of data for storage into internal storage A
internal storage B
aPPb
Smart-Phone B

FIGURE 1: Memory Sharing – Data Exchange from Smart Phone B to Smart Phone A

As it can be seen from the figure 1, a one to one scenario is being reflected where two devices are communicating over the cloud server which mitigates for proximity communication over connectivity solutions such as Wi-Fi, bluetooth, or NFC etc. here the cloud serves the medium within these connected nodes such as smart phone devices.

For data transfer and retrieval, there is an application or user interface module which ensures the data transfer in an unused memory of a secondary device. This module might have some designated contacts which can have their credentials checked for drag and drop request generation and quick transfer of data. Once the user of a device which needs to transfer some amount of data to a third party (a family or a friend or a designated contact) drags that particular contact into the data retrieval and transfer app and the activity gets marked for data transfer process. This drag and drop action generate an upload request by enabling an upload feature on a user interface module and initiate uploading of selected items on the cloud storage.

In this internet savvy generation, this approach of data transfer need to be made secure as well using the encryption mechanism or authentication using password or keys, in order to protect your data from being modified or fabricated. Data encryption provides high security to prevent access to file contents and ensure clients privacy against the NSA.

For secure transmission and encryption of data, this approach uses most powerful spying tool of NSA i.e. encryption keys of mobile SIM card for encryption. These keys are also present on the mobile network; are kept carefully protected in the core network. These keys are used to authenticate subscribers on mobile telephony devices. There are also several other ways for encrypting data in transmit for example 256 AES encryption or IPSec VPN or group encryption solution.

Ensure that data must be encrypted or before it is sent to cloud server storage. The encryption of data is done at user's side. The key used for encryption algorithm is generated in the user environment. Once upload is complete, cloud server notify the selected contact to download the data. On acceptance of the request, data starts downloading on the device of selected contact.

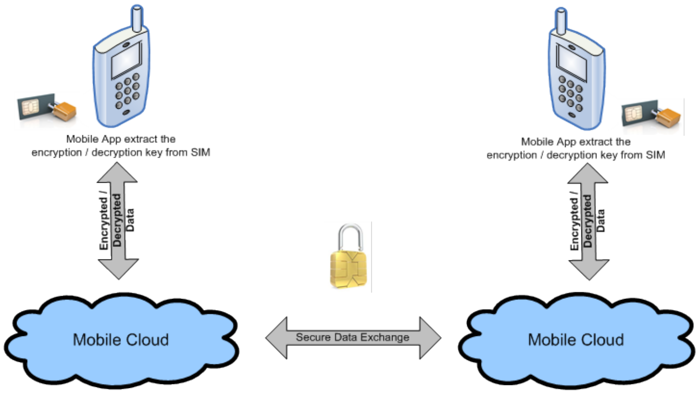
Mobile App extract the encryption / decryption key from SIM
Mobile App extract the encryption / decryption key from SIM
Encrypted / Decrypted Data
Encrypted / Decrypted Data
Mobile Cloud
Secure Data Exchange
Mobile Cloud

FIGURE 2: Secure Data exchange between smart phones using SIM key encryption.

As it can be seen from figure 2, SIM key is used by applications on smart phones to encrypt or decrypt the data for secure data exchange over cloud storage. The application on device requests the SIM application for ciphering key generated using ciphering algorithm to encrypt or decrypt the data. The computation of ciphering key takes place internally within the SIM. To make system more resistant to eavesdropping, GSM provides an additional level of security by having a way to change ciphering key at regular intervals.

After successful data transfer of encrypted data, issuer of the request can ask secondary device for getting its data back in device i.e. request of data retrieval as and when required. This data retrieval happens the same way data upload takes place. Secondary device upload the data back to the cloud server and issuer of the request downloads it from server as long as data upload on server finishes and decrypts it the same way as it was encrypted using ciphering key.

In general, each smart device has a set of designated contacts in their respective data retrieval or transfer app, each of the devices can request any of the designated contacts to store their data in their unused storages.

III. CONCLUSION

Internal memory sharing between smart phones offers secure and efficient system to upload or retrieve data to or from other trusted smart phone devices without any loss of data. It provides users a cost effective way of expanding their internalstorages with use of unused memory of other phone devices to store their unlimited data. This proposed technique provides confidentiality to the user's data by using encryption technique which prevents user data from being modified or fabricated. Additionally, this technique protects your data from being lost by storing it to smart phones of trusted contact.

REFERENCES

1. L. Arockiam , S. Monikandan, "Efficient Cloud Storage Confidentiality to Ensure Data Security" in 2014 International Conference on Computer Communication and Informatics (ICCCI -2014), Jan. 03 – 05, 2014, Coimbatore, INDIA
2. https://www.wikipedia.org/

AUTHORS

First Author –Surbhi Gupta, Masters of computer applications, surbhigupta0189@gmail.com