

## SHARING SECURE FILES USING NFC CLONE TECHNOLOGY ON ANDROID DEVICES

ARPANA MEHLA 1, TANU SHARMA ANGRA 2, VINEET GOYAL 2, VIKAS 2

1 Student,ChitkaraUniversity,H.P

2 Assistant Professor,Chitkara University,H.P

2 Student,ChitkaraUniversity,H.P

2 Student,Chitkara University,H.P

**ABSTRACT:** In this paper we are artificiating NFC technology to share files among two devices .NFC (NEAR FIELD COMMUNICATION), is a technology used to share data or files among devices supporting it. The big plus of NFC is, it makes sharing very easier for users, which happens just by touching two devices and file is transferred. This is to implement same concept using Bluetooth technology. The notion is to implement it using accelerometer, in accelerometer powered android devices. When two android devices are touched, application detects accelerometer's activity of the device which are touched and stores respective timestamps in devices. After matching the timestamps of the two devices tucked , the required file will be sent to the respective device.

**KEYWORDS:** Accelerometer activation , Artificiating NFC, Auto bluetooth matching ,Gallery access, File sharing, Timestamp matching , MD5 encryption.

### INTRODUCTION:

Near-field Communication or NFC is a standard defined by the NFC forum, and is a short-range radio technology that operates on 13.56MHz frequency with data transfer of 424 kilobits per second.NFC communication is done when two NFC enabled devices are brought together in a close proximity, or touched together. But there were some shortcomings of this technology, which are listed below:

- Equipment Required
- Cost

- Understanding
- Technical Limitations

In order to overcome these problems, the concept of Artificiating NFC technology came into mind so that some of the similar advantages can be explored and eliminate the cons.

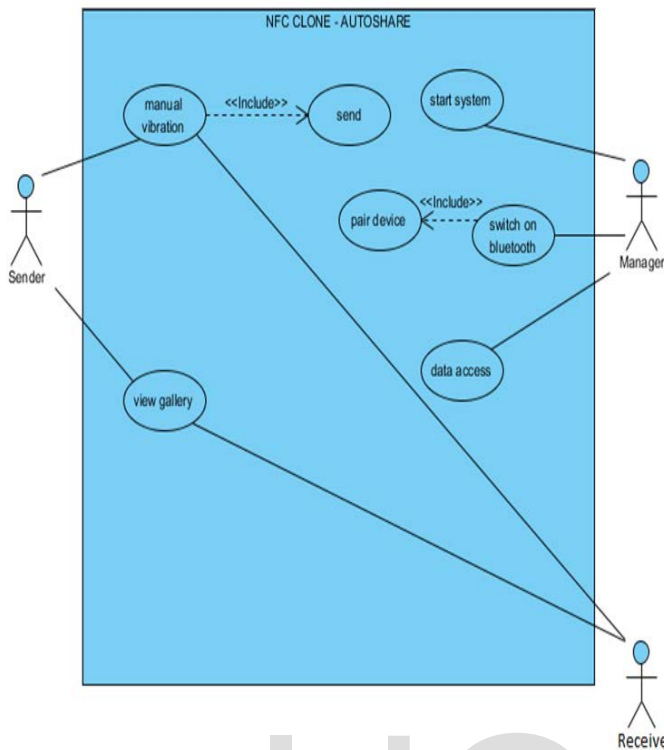


Figure 1: Use case diagram of NFC Clone Autoshare

Whole work is done in modules. These modules are listed below:

1. Gallery Access
2. Auto Bluetooth Management
3. Accelerometer Activation
4. Algorithm For Vibration detection
5. Timestamp Matching
6. Bluetooth share
7. MD5 Encryption

All the modules stated above have their own designated role to play, which are very pivotal for smooth and expected functioning of application with a lot of reliability. As every module is designed to perform a specific task necessary to obtain objective of application, all the modules stated above are well defined in detail with all the associated algorithms. These modules start their operations at particular activity instants, that is they execute only when function required is to be performed and shift operations to other modules after their job is done and thus stop their execution, which makes this application very battery efficient, specially with module which is responsible for accelerometer activation.

### MODULE – 1: GALLERY ACCESS

This module is responsible for access to file system of device. File system in android powered devices is managed by operating system itself. Accessing that file system and showing in application window while making it easy for user to understand the interface is coded into this module. This module is first module which executes if user is not in Receive-Only mode as to send a file via Bluetooth the very first requirement is that the file to be shared must be selected and for selecting one file among many, user needs to be provided with options of directories and

files available to choose from. Logical presentation of various directories and files present therein is done via this module. Touch on directory opens it to view files present in it and touch on file opens it for view and initiates execution of other modules. Selection of file acts as activity instant for other modules to start execution.

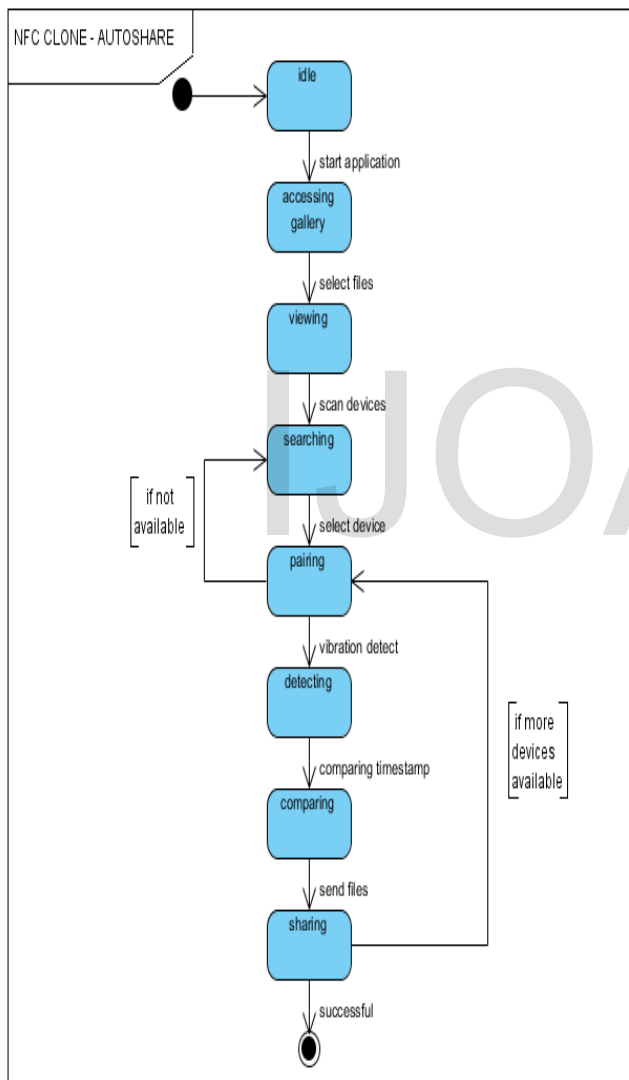


Figure:2 State machine diagram of NFC Clone Autoshare.

## MODULE – 2: AUTO BLUETOOTH MANAGEMENT

This module contributes in our final effort to make whole sharing process via Bluetooth very easy. This Module is responsible for automatically switching on Bluetooth, switching it off, selecting appropriate device, authenticating share process. This module does it all by itself without any interference of user. This module is the key module in making this ideological application implementable and realise its function. Bluetooth is an open system so it can have some security risks. In today's world a lot of mobile phones and other different devices include Bluetooth and in some cases the people who buy those devices don't know even that the Bluetooth system is operating. There are some opinions which say that Bluetooth is unsecure in the encryption and some other technical aspects but most of the information we found about Bluetooth security is quite technical. That's why we are using MD5 algorithm for security to make sharing process more secure.

## MODULE – 3: ACCELEROMETER ACTIVATION

This module is about activating accelerometer only when it is required and that too without human intervention. It activates accelerometer when file is selected and made to view as only after appropriate file selection share can be initiated. And after viewing is terminated Accelerometer is deactivated again.

## MODULE – 4: ALGORITHM FOR VIBRATION DETECTION

Very important and key module of application which makes whole idea actually implementable. This module detects when mobile device is tugged with another mobile device or detects when mobile is bumped into another mobile device.

### CONCEPTUAL LOGIC – ALGORITHM

- 1) Value for acceleration is checked every 200 millisecond
- 2) Then difference between consecutive values is computed
- 3) Then absolute of that difference is compared with 3
- 4) If Modulus of difference is more than three
- 5) Return vibration detected
- 6) Else continue computing every 200 milliseconds

This algorithm works very efficiently for vibration detection eliminating absurd results obtained because of acceleration due to gravity.

Example :

Computation:

$X = (\text{Acc. value at } 0 \text{ ms});$

$Y = (\text{Acc. Value at } 200 \text{ ms});$

$\text{Diff} = \text{absolute}( X - Y);$

If( Diff > 3)

{

Return(“vibration detected”);

}

Else {continue computation};

## MODULE – 5: TIMESTAMP MATCHING

As sharing via Bluetooth requires authentication to check which mobile device we need to send data to. For appropriate device selection we have devised a unique algorithm, that is time stamp matching. System stores value of timestamp when vibration is detected and then is matched with the value stored in other device. If match returns true, share process starts else match with other device or record new timestamp. This module is another very key element of this application as this is the module which saves the user overhead of selecting device to be sent to.

## MODULE – 6: BLUETOOTH SHARE

After all the modules have returned result expected out of them Bluetooth Share is called. Which is responsible for transfer of data to another device. It sends data to Bluetooth Mac returned after timestamp matching.

## MODULE – 7: MD5 ENCRYPTION

To solve very intricate issues of security while sharing data with this application we are using MD5 encryption algorithm. MD5 algorithm is used as digital signature mechanism. This application will encrypt the core confirmation technique so as to make sure device it is sharing with is appropriate. Timestamp recorded is encrypted with MD5 before sending it to device for confirmation .It will take a message of arbitrary length and will produce an output of 128 bit message digest or hash value of the input message. The input message is then divided into 16 32- bits words. And then the message is padded so that its length is divisible by 512. At the other end also timestamp recorded is again decrypted using same technique. This will make share process a lot more secure in terms of selecting device to send data to.

### CONCLUSION:

The research work has been completed successfully, tested as well as implemented as an application to the Android Operating System currently being implemented for mobile devices. With the help of this application, we will be able to send images to other phones easily without much effort and without checking for the enable/disable bluetooth or the usual confirmations which occur for the file sharing.

### FUTURE ENHANCEMENTS:

In future we can make enhancements in the graphics, besides adding of more functionality we will try to

protect user files with the help of password security system. Also speed of transfer can be increased.

### REFERENCES:

- [1] Ed Brunette. Hello,Android Introducing Googles Mobile Development platform. 3<sup>rd</sup> ed. Pragmatic Publication; 2010
- [2] Robert Schildt. The Complete Reference Java .5<sup>th</sup> ed.Tata McGraw Hill publication; 2011
- [3] Marko Gargenta. Learning Android.1<sup>st</sup> ed.O'Reilly Media publication;2011
- [4]Abraham Silberschatz, Peter Baer Galvin,Greg Gagne.Operating System Concepts.7<sup>th</sup> ed.John Wiley and sons publications;2006
- [5] Mateja Jovanovic, Mario Muñoz Organero Analysis of the Latest Trends in Mobile Commerce using the NFC Technology,may 2011
- [6][http://www.appszoom.com/android\\_applications/research+papers](http://www.appszoom.com/android_applications/research+papers)
- [7]<http://libguides.mit.edu/content.php?pid=174869&sid=1481864>
- [8]<http://www.jite.org/documents/Vo12/JITEv6p481-497Philip295.pdf>
- [9] Ortiz, C. Enrique (2006-06). "An Introduction to Near-Field Communication and the Contactless Communication API". Retrieved 2008-10-24
- [10] Kasper, Timo; Dario Carluccio, Christof Paar (May 2007). "An embedded system for practical security analysis of contactless smartcards" (PDF). Springer

LNCS (Workshop in Information Security Theory and Practices 2007, Heraklion, Crete, Greece) 4462: 150–60

[11] <http://bluetooth.com/Bluetooth/Technology/Works/Security>

[12] Bert den Boer, Antoon Bosselaers (1993). "Collisions for the Compression Function of MD5". EUROCRYPT. Berlin; London: Springer. pp. 293–304. ISBN 3-540-57600-2.

IJOART