INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SECURE FILE TRANSFER FOR ANDROID USING DES ALGORITHM

ASST. PROF. AKSHAY D. ISALKAR, MISS. DIPEEKA D. BORKUTE, MISS. DIKSHA D. KASATWAR, MISS. ANKITA A. AGRAWAL, MR. WASIM A. SOLANKI

Dept. of Information Technology, DMIETR, Wardha-442001

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract: Now a day in this world nothing is secure. In all fields there is confidential data, and it should be secure. The data should not get hacked by the hackers or anyone who will misuse the confidential information. To protect such kind of information some security mechanism is available. Password is commonly used technique to secure our data. In this paper we are designing and developing an application which provides security for transferring the file/data with the help of DES algorithm, where it encrypts and decrypts the data with the help of secret key, here transmission is done in two ways, If the file/data is public then file is selected and sent to particular receiver, if the file/data is private it ask for security key and send towards receiver mobile number then receiver decrypt this file using this secret key, this way we achieve the secure transmission of information (file/data) between end-users.

Keywords: DES (Data Encryption standard), Encrypted File system, Secret Key.

Corresponding Author: MR. WASIM A. SOLANKI

Access Online On:

www.ijpret.com

How to Cite This Article:

Wasim A. Solanki, IJPRET, 2016; Volume 4 (9): 107-113

PAPER-QR CODE

INTRODUCTION

We propose an android application that ensures the user that confidentiality to his/her data. Every android phone has a limit to the store the data into it, and thus when the data stored in the system gets overloaded needs to be transferred to a better and trustworthy system. As no system on its own is trustworthy so there leakage a need to make it secure using some application, hence an android application which works on the concept of DES algorithm with secret key , transfers the data into an encrypted format via Wi-fi. In this paper we are designing and developing an application which provides security for transferring the file/data with the help of DES algorithm, where it encrypts and decrypts the data with the help of secret key, If the file/data is public then file is selected and sent to particular receiver, if the file/data is private it ask for security key and sent towards receiver by using the receivers mobile number then receiver decrypt this file using this secret key, this way we achieve the private transmission of information (file/data) between end-users.

PROPOSED WORK

In our proposed system two hardware's are used which are two android based smartphones, with the help of which Users can transfer any kind have to open the sender application and have to select the file or the data which has to be sent towards the another end user, and the end users also should open the receiver application. Once the application opened in the sender's android smartphone the application will automatically search for the IP's in existing Wi-Fi range and list all the existing Wi-Fi based android smartphones IP's. Sender has to select the particular IP-address's among the list of existing devices browse the file and transfer to the desired receiver end.

A. DES ALGORITHM:

The data Encryption Standard (DES) is also called as Data Encryption algorithm (DEA) by ANSI and DEA-1 by ISO has been cryptographic algorithm used for over three decades.

B. WORKING OF DES:

DES is a block cipher. IT encrypts data in a block size of 64 bits each. That is, 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text. The same algorithm and key is used for the encryption and decryption, with minor differences. The key length is 56 bits.

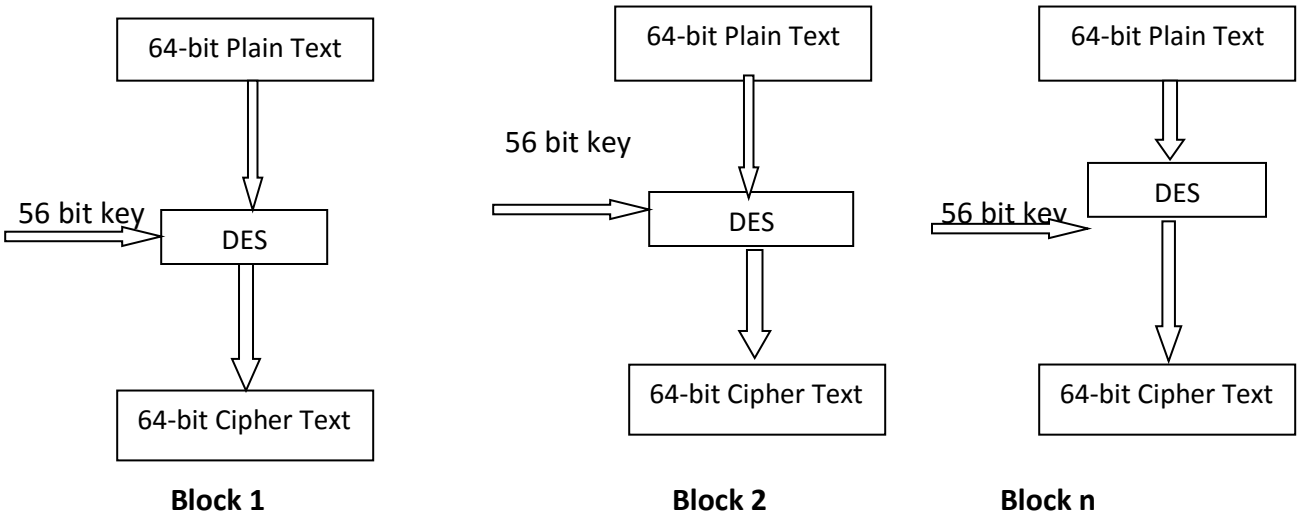

Fig 1: The conceptual working of DES

C. BROAD LEVEL STEPS IN DES:

1. 64-bit plain text block is handed over to an Initial Permutation (IP) function.

2. The Initial Permutation is performed on plain text.

3. The Initial Permutation produces two halves of the permuted block: Left Plain Text (LPT) and Right Plain Text (RPT).

4. Now, each of LPT and RPT go through 16 rounds of encryption process.

5. In the end, LPT and RPT are rejoined and a Final Permutation is performed on the combined block.

6. The result of this process produces 64 bit cipher text.

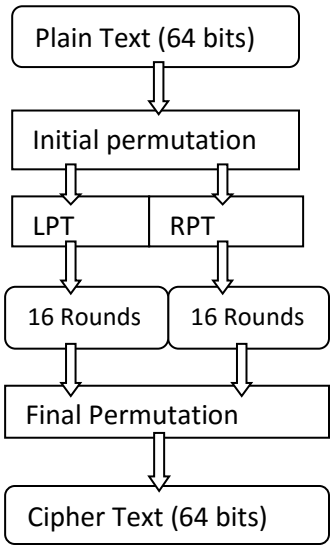

Fig 2: Broad Level steps in DES

SYSTEM DESIGN ARCHITECTURE

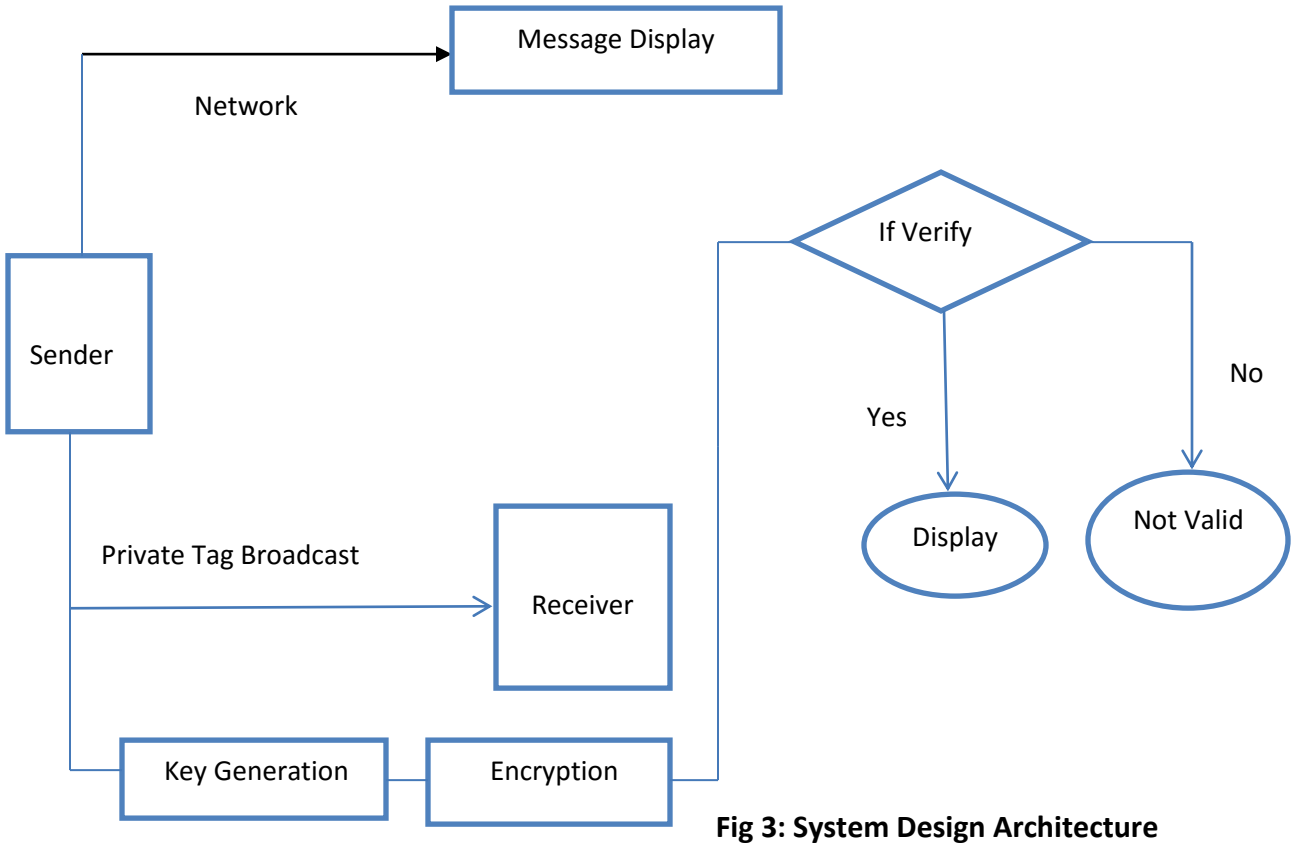

Fig 3: System Design Architecture

The above diagram represents the system architecture, the main components of the system are android devices or android smartphones, transfer mode, GUI, encryption, decryption, scan IP, and random key generation. Here android based devices or smartphones with Wi-Fi are used as hardware which works as sender and receiver in which the user should have installed with relevant applications on their devices

IMPLEMENTATION

The implementation of application is developed using the java programming in eclipse framework. The architecture can be implemented using the followings

- Programming language: Java, XML
- Frame work: Eclipse
- Supporting tool: Android SDK
- Platform: Windows XP/Vista/07/08

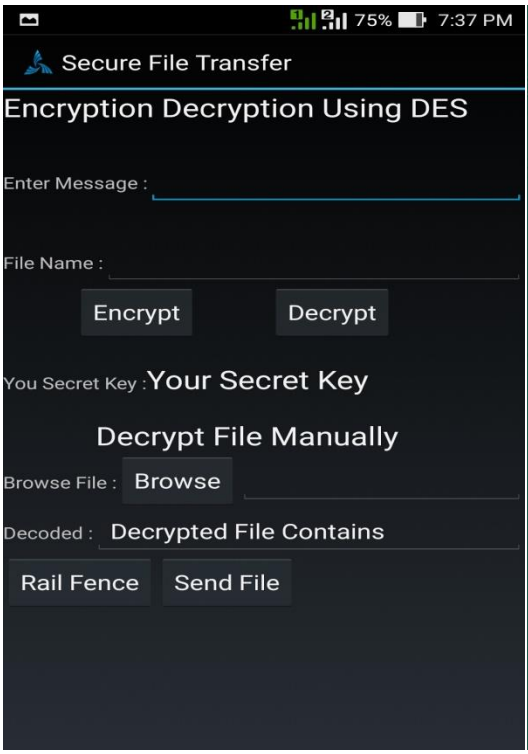

Fig 4: Generate Secret key

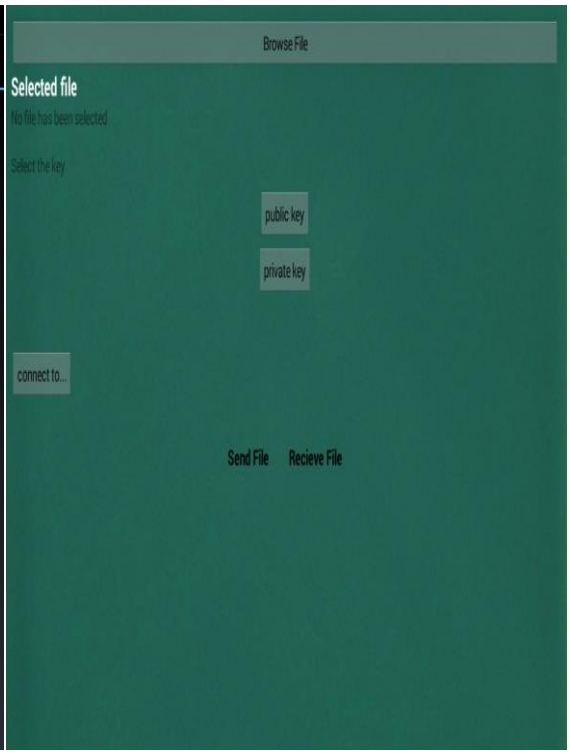

Fig 5: Select Mode

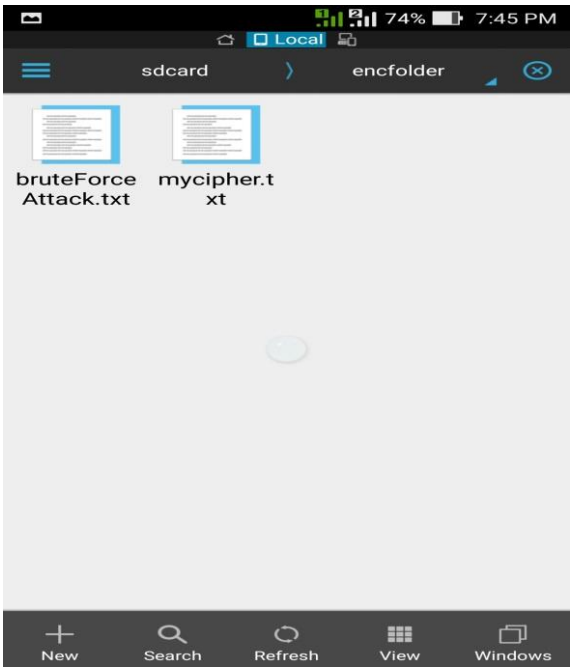

Fig 6: Select Folder **Fig 7: Obtaining Cipher text**

CONCLUSION AND FUTURE SCOPE

The proposed android application enhances the authentication over the system and Wifi sharing experience by making it more secure. Hence textual password scheme is user friendly and more secured. This system also provides more scope in concern of the authentication. This system is proposed using Wifi which can further enhance to more efficient way that is using network. In future our proposed work is very help full to increase the security included graphical password it provides more security. also used as an online application and developed such type of Application for system by using systems IP address and we send a file like audio, video, graphical files, images etc.

ACKNOWLEDGMENT

Author would like to give his sincere gratitude to guide Mr. Akshay D. Isalkar who encouraged and guided us throughout this paper.

REFERENCES

1. Tayyaba Tamboli1, Sayli Raut2, Rohini Musale3(2014) "A Novel Approach for Authentication in File Transfer Using Bluetooth" IJETT ISSN: 2350 – 0808 September 2014| Volume 1 Issue 1

2. Zhaohui Wang (2012) "Implementing and Optimizing an Encryption File system on Android"- DOI 10.1109/MDM.2012.3

3. *Ajita A. Mahapadi (2015)* "F-Share for Hand Held Devices Using Wi-Fi Bluetooth Network"- IJERT Volume: 02 Issue: 03

4. Dattatreya Hadapad (2013) "Android Application For Secure File Transferring using Data Encryption Standard"- IJERT

5. Daniel Camps-Mur, Andres Garcia-Saavedra and Pablo Serrano(2013) "Device to device communications with WiFi Direct: overview and experimentation"-IEEE

6. Androidsecurityoverview,"http://source.android.com/tech/security/index.html.[Online].Available:http://source.android.com/tech/security/index.html

7. Xue Zhang Cheng, Wu shunxiang, "File Transferring via Bluetooth using obex protocol", Wireless Networks and Information Systems, 2009

8. John Oates (15 June 2004). "Virus attacks mobiles via Bluetooth". The Register. Retrieved 2007-02-01.

9. "Whisper core android device encryption," http://whispersys.com/whispercore.html.

10. Android Project. http://www.android.com.

11. Yajin Zhou, Xinwen Zhang, Xuxian Jiang, and V.W. Freeh. Taming Information-Stealing Smartphone Applications (on Android). In *Proc. TRUST 2011*, 2011.to be published.

12. Gartner says android to command nearly half of worldwide smartphone operating system market by year end 2012.http://www.gartner.com/it/page.jspid=1622614.