File Hider – An Android App for Proficient Secured File Storage

Pranava G R
Student of IV Semester,
Department of MCA
R.V. College of Engineering,
Mysore Road, Bengaluru-59, Affiliated to VTU, Belagavi

Manish B V
Student of IV Semester,
Department of MCA
R.V. College of Engineering,
Mysore Road, Bengaluru-59, Affiliated to VTU, Belagavi

Andhe Dharani
Professor, Department of MCA
R.V. College of Engineering,
Mysore Road, Bengaluru-59, Affiliated to VTU, Belagavi

***Abstract*- The amount of data processed and stored from various devices across the globe is on the threshold of thousands Exabytes and is increasing as per the second. Day in and day out users are storing various personal, official related data on their mobile devices. Any file stored either in the internal or external storage is in need of protection. Hiding data as well as ensuring the effectiveness in transfer of files is the objective of the work carried out in this paper. This paper deals with the app created to encrypt and hide the files for storage on internal devices as well as decrypt based on the requirement and authentication.**

I. INTRODUCTION

Now-a-days Android smart phones are became popular and inseparable part in one's life through the outstanding features. As per literature and it is said that by 2020 the percentage of the total IP traffic by PCs will account for only 29 percent whereas the IP traffic from Smartphones will account for 30 percent, which in 2015 is only 8 percent from Smartphones [1].

In recent years, mobile phones have been changed by the emergence of smart phones. It is no longer just a communication tool, but also become an essential part of the people's daily life. Mobile subscriptions are growing around 3 percent year-on-year globally and reached 7.4 billion in Q1 2016. India grew the most in terms of net additions during the quarter (+21 million), followed by Myanmar (+5 million), Indonesia (+5 million), the US (+3 million) and Pakistan (+3 million) [2].

Various applications of android provide fun and other needs of daily life. Personally owned smartphones and tablets, like desktops and laptops, have become a standard work tool [3]. Many companies are implementing the "bring your own device movement", which will help in increasing productivity and ensuring recognition of the devices.

The major problem with this may be that the users tend to have official files / folders which might need security. Without proper security like encryption and enforcement of password the data might be at a huge risk as users tend to do work from home also.

The majority of the problem when unintended users like spouses or kids or any other persons uses the smartphones or tabs. The chances of them deleting or altering the contents are of a great risk. The user might need to secure it by encrypting as well as hide some files.

This paper gives an working solution for users who can access their data securely and ensure that any unintended users are not going to tamper with them by hiding and encrypting the data files or folders

II. FUNCTIONALITY

This work deals with the app which not only gives the security but also records and send the information of the persons who try to access it. The information is sent as an image captured when entered wrong passwords and also send it to the registered email id for verification. The security is given by encrypting, giving option to hide the encrypted files from the usual set of files. Apart from this an One Time Password (OTP) authentication is done to verify when any password mistake has happened during entry. Many other file features are also provided as a part of the working procedure.

The work carried out is in different modules based on the working functionality. Below in this section describes the different functionalities carried out.

A. Interactive File Explorer:

It explores the File System of internal and external storage for selecting directory and files to Hide and Encrypt. It also shows Animated Icon for Files and some Folders

B. Encryption:

Hidden File/Directory are Encrypted so that no one can understand Files. It adds some salt to the original content and encrypts using Hash.

C. File Hide:

The Encrypted File/Directory is hidden in a secure Location. Currently the location used is the predetermined by the android OS structure. That is it creates the hidden folder in Android/data and stores all encrypted files. More security can be thought of if the structuring can be changed based using another algorithm.

D. Unique Name

The encrypted file is stored with unique name. Auto generation of the name has been carried out to ensure that repetition of the name after encrypting for hiding is not

feasible. This ensures there are no clashes even with any number of files.

E. Decryption

The Encrypted File/Directory is decrypted and separates the salt from original content.

F. Password Recovery/ OTP Generation

User can recover the forgotten password after OTP verification. In the time of Password Recovery it generates the random One Time Password (OTP) and sends to user's registered Email Id to check Authentication of the User. One time password is the best way of any authentication.

G. Handling Hack Attempts

The application captures the photo with date and time and stores it in "Android/data/.com.quadcore.capture" when someone tries to open application for 3 times with wrong password and it sends that photo to registered User's Mail Id when internet is connected. Any hacker or unintended users, tries to open application for 3 times with wrong password the application will lock itself for some time. This time will increases when another set of wrong Password entered. The time gaps is utilized for sending the photo message to registered mail id and notify for any discrepancies. It checks the internet connection using Ping.

H. Other Operations:

Selected File/Directory can be permanently Delete by the File system. The File/Directory can also be Rename according to the User. User can change the password according to time by using the Old Password.

I. Other Features:

Toast messages and older data: This Application shows the proper toast time to time. When app is minimized the state is stored in Shared Preference, after login app comes back to its older state.

Email Id Format checker:

It checks the format of Email Id, if format is correct then only it allows to register.

III. RELATED TOOLS AND TECHNOLOGIES

The tools and technologies utilized in the development of this app are described in this section.

Android

This era is very great and exiting for mobile developers. Android provides a very good foundation towards developer's ideas. Android is an open source platform that includes operating system, application framework, Linux kernel, middleware and application along with a set of API libraries that will provide looks, feel and function of mobile handset and also provide rich tools to make interactive application. Downloading the software's required for making the application are absolutely free [4].

According to survey there is 70-85 % of the people familiar with the android device, in than 95% are youngsters and remaining 5% of the peoples are elders but day by day it will help to all of those to work with it.

The majority of the youngsters are the ones who need to have hide the files for protection.

The Major classes used in this work is as follows –

- Capture Activity: To capture the activity screen area of android app.
- ChangePasswordDialogFragment: Dialog box for providing password changing facility.
- Crypt : Crypto function to encrypt the password
- DatabaseHandlerFile & DatabaseHandlerUser: To handle list of usernames and password
- FileArrayAdapter , FileAttributeHolder, FileExplorer, FileHiderService : File attributes and other services with respect to the File stored on the android services
- Hash: To encode the password using hashing functions
- HideList , HideListArrayAdapter- List of items or files hidden with its attributes.
- Item : Files or Folder
- LoginActivity, RegisterActivity – Class to functions on user registration and creation procedure.
- Mail services mail e-mail notifications.

IV. RESULTS AND CONCLUSIONS

The output of the work is to provide reliable secured storage of data in files or folders for users. Below gives the output screen shots of the working process carried out.

Outputs:

Figure 1 – Splash Screen

Above figure 1 depicts the entry screen. This is the Splash Screen window contains an image. This is used to notify the user that the program is in process of loading. This window disappears when the application's Login/Register window appears. The screen has been provided to enhance the look and feel of the application.

Figure 2 – login sceen

If user enters invalid Password the app will show a toast which contains Invalid Password. An user needs to register themselves for the application and then can access it. They can hide/unhide, encrypt/decrypt the data. To do any functionality they need to register themselves first. After entering wrong password each time the time limit elapses. The time setting decreases and the counter clock time is kept clicking as shown in figure 2 below making it difficult for brute force hackers to think and hack.

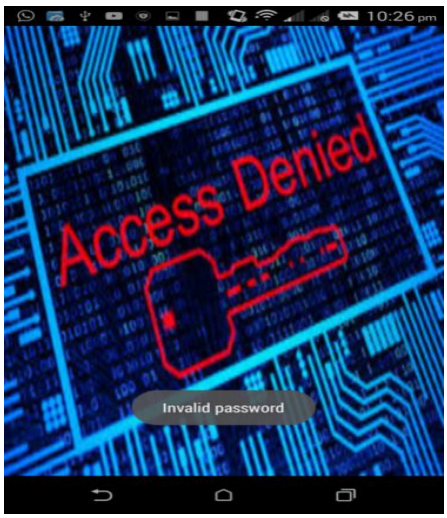

Figure 3 – Invalid attempts

If the correct password is not given in the time limit the system locks. Figure 3 depicts the screen after locking on not entering the correct passwords within the stipulated time. Three chances for a given time limit is permitted so as to ensure thinking for brute force hacking time is less. Along with locking of the screen, the application secretly captures the photo of that person. [if and only if device has front cam].

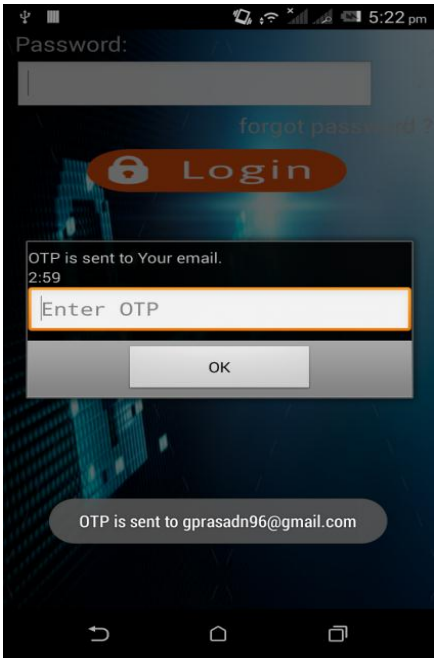

Figure 4 –OTP request response

If on blocking if an user wants to unlock, to retrieve his files on the mobile, the user can send in an request or an OTP is generated to the registered mail id, the user needs to have the mail data on as the OTP is also given under limited time for security reasons.

Figure 5 and 6 shows the different operations that can be done on the files. If user touch and holds some file/folder, a dialog will appear with four file options as shown in figure 5. If user selects Hide option the respected file/folder will encrypted and then hide in secret location. This will be done after confirmation again with a message. Apart from hiding the user can do other operations also. If the user want to retrieve the hidden file the user can do so by clicking on the unhide option which is listed under the option menu on the top left side of the mobile screen. When selected the user will be shown with the list of hidden files and they can check out which one needs to be hidden. The path of the files hidden is by default in the coding done in the app and for further security can be hidden from the user and only the contents retrieved when needed. The major aim of this work proposed in the paper is about ensuring that the files / folders can be given security on mobile phones and the same can be adapted for tabs also. This is becoming a high need as the usage of the data is as done on PC in the next coming years, but the misuse of the same based on the size of the gadget is more compared.

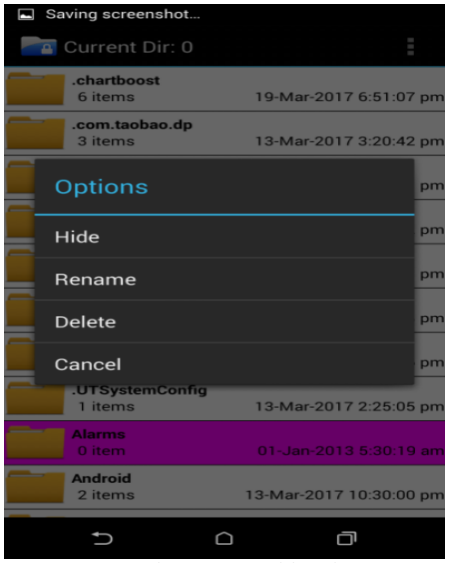

Figure 5 – Screen for selection of files for operations

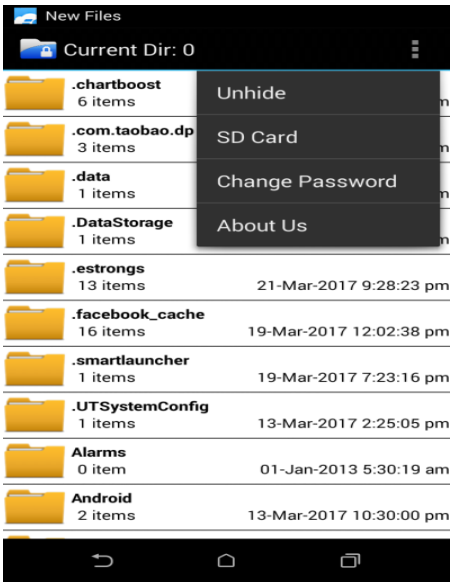

Figure 6 – Screen for selection of files for operations

REFERENCES

[1] Cisco “The Zettabyte Era — Trends and Analysis”, Document ID:1465272001812119, June 2, 2016
[2] Ericsson, “Ericsson Mobility Report”, ON THE PULSE OF THE NETWORKED SOCIETY, June 2016
[3] Dell “Transparent data protection for smartphones and tablets” Dell Data Protection | Mobile Edition
[4] Akshay Singh, Shakshi Sharma, Shashwat Singh “Android Application Development using Android Studio and PHP Framework” International Journal of Computer Applications, 2016,pp 0975 – 8887

Programming Reference Materials:

[5] Android Developers, [Online], Available at URL: [https://developer.android.com/reference/javax/crypto/interfaces/package-summary.html], accessed on [12th May 2017]
[6] Android Developers, [Online], Available at URL: [https://developer.android.com/reference/java/lang/Class.html] , accessed on [10th May 2017]
[7] Android Developers, [Online], Available at URL: [https://developer.android.com/reference/java/lang/reflect/Method.html], accessed on [10th May 2017]
[8] Android Developers, [Online], Available at URL:[https://developer.android.com/reference/android/database/package-summary.html], accessed on [12th May 2017]
[9] https://in.udacity.com/course/new-android-fundamentals--ud851/, accessed on [12th May 2017]