International Journal of Undergraduate Research 2 (2): 30-33, 2020
e-ISSN: 2682-8189

DOI: 10.26666/rmp.ijur.2020.2.5

Secured File and Data Storing with Self-Encryption and Location Tracking in Mobile Application

Nurul Husna Abd Aziz, Nor Fazlida Mohd Sani, Noor Afiza Mohd Ariffin.
Department of Computer Science,
Faculty of Computer Science and Information Technology
University Putra Malaysia, Selangor, Malaysia.

186783@student.upm.edu.my, fazlida@upm.edu.my, noorafiza@upm.edu.my

Abstract : Mobile phone has become a very important asset to people and most people have one on hand at all times. Mobile phone has been considered a blessing as it has many capabilities and is not just limited to calling and text messaging. Every people will use mobile phone as a device to save their important data or to perform any transactions. This is because the mobile phone is a handheld device and easy to bring anywhere. As mobile phones are becoming more popular and the prices are rising in the market, the probability of missing or stolen mobile phones is also increasing in society. To overcome these issues, this paper introduces a new mobile application named Secured File and Data Storing with Self-Encryption and Location Tracking, which capable to increase the security of the user's data by integrate with fingerprint authentication, secure data in the encrypted format can retrieve back the loss of data and can track the lost mobile phone location.

Keywords: *Self-Encryption, Location Tracking, OTP*

Introduction

Data protection is the process of safeguarding important information from misuse, compromise or loss[1]. Data has become more and more valuable nowadays. The skills, expertise, and opportunities to retrieving different types of personal data are evolving extremely fast. Unauthorized, careless or ignorant processing of personal data can cause great harm to persons and to companies[2].

The convenience of technology on mobile phones makes people use their phones for everything including store their important data or business transaction on the mobile phone. Mobile phone shows a drastic result in technology change makes people use a mobile phone as their important asset. The statistic shows the total number of mobile phone users worldwide from 2015 to 2020, in 2019 the number of mobile phone users is forecast to reach 4.68 billion[3]. The possibility of mobile loses or be stolen are increased due to the mobile phone price in the market.

In this project, the proposed system would give a huge benefit to mobile phone users to secure their confidential and private data in a secure way. This system provides the authentication layer to allows only authorized users can enter the system and location tracking to track phone location.

Literature Review

Mobile Self Encryption, Gurdhalkar et al. (2018).

This paper proposed a system that concentrates on securing the user's data on the devices using encryption algorithms for security purposes and stored the data in an encrypted format. In this system, the data are encrypted using a secret key that only allow authorized user to access the data. This system protected the data from the malicious user. Even if malicious users got to access the online

Corresponding Author: Nurul Husna Abd. Aziz, Department of Computer Science, Faculty of Computer Science and Information Technology, University Putra Malaysia, Selangor, Malaysia. Email: 186783@student.upm.edu.my

database, they will not be able to get the real data because the data is stored in an encrypted format which is not understandable. If the mobile device is lost, the system will send a report to a server and the server then destroys the respective key. Data on that lost mobile can never be decrypted and remains confidential from unauthorized persons. This existing system uses cloud storage that allows the user to access the data by login to the system using another mobile device. The AES (Advanced Encryption Standard) algorithm in this system will give the system a slow performance for encryption and decryption process due to the key size. In the transition of time, AES algorithm has been proven to be a weak cipher. [4]

Mobile Self Encryption System, Jagtap et al. (2019).

This paper proposed a system that store user data from mobile to a server and for security data will be encrypted form and while at the time of data access user have to enter OTP and decryption key then the only user will get the file. The key and OTP will get on the user's second mobile number that is given at the time of registration. If the key matched user will get a decrypted file. If the user's mobile device is lost then there is no issue to access stored data on a server. Users will get the file from anywhere. The proposed system increases data security for the user's mobile data. The proposed system is developed in the Android platform. [5]

Anti Theft Mobile Tracker Application. Deebika.T et al. (2016).

This paper proposed a system that uses to GPS (Global Positioning System) service to track the location, front camera to capture images and sending a message to the registered phone number of the phone location and then the image of a person is captured and send via email. This system allows user to delete all the data stored in the database in this application. The role of the user in this application is to set the mode as safe when he changes the SIM (subscriber identification module) card and to send SMS (short message service) to the Android Smartphone having this application installed in it when it is stolen or lost.[6]

Folder Lock by NewSoftwares LLC.

This application lets the user password-protect personal files, photos, videos, documents, contacts, wallet cards, notes and audio recordings in Android Phones. The app comes with a clean and pleasant interface. Users can also transfer files from Gallery, PC/Mac, Camera and Internet browser. This application provides lock photos with photo locker to hide user images**,** lock videos with video locker to hide user videos**,** gallery lock vault to hide user albums**,** notes lock to lock and hide user notes and lock apps to prevent access to user private app lock. However, this application did not have an encryption technique for file store. It is secured the file using the authentication security technique which is pin and fingerprint but the fingerprint authentication only works for paid user. [7]

ZenCrypt - Securely Encrypt Files by Zestas.

ZenCrypt is an all-in-one encryption app, which allows you to encrypt and decrypt files and folders with one click. It will protect user private data using AES 128 algorithm. The key generation is a random key generation with the updated generation code recommended for Android. This application did not provide authentication to free users and provides fingerprint authentication for paid users. User needs to remember the encrypted key that they insert in order to decrypt the file. [8]

Methodology

In this system development phase, the Agile Software Development Life Cycle has been used to design, implement and test the system. There are four important phases:

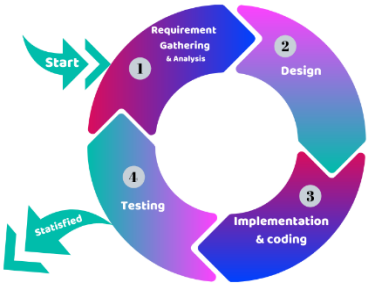

Figure 1: Agile Software Development Life Cycle

Agile methodology is a practice that promotes continuous iteration of development and testing throughout the software development life cycle of the project where the development and testing activities are concurrent[9].

Requirement Gathering and Analysis phase is the planning phase for the quality assurance

requirements and identification of the risks. This phase required to analyses the system needs. The requirement will be analyses to decide what encryption technique and programming language should be used. In this phase, the requirement of the system is state and analyze in the Software Requirement Specification document. For this project, to define that the final product meets expectations, the following are the parts that will be completed:

- Secure system with fingerprint authentication.
- OTP (One-Time Password) is needed every time the data is decrypted.
- Can track the location of the mobile phone.

For maintaining the robustness of the system, the system should ensure following in the project:

- Overall system quality should give a smooth experience for users.
- The system can encrypt and decrypt the data when needed.
- Only authorized users can login to the system.
- The system can locate a mobile phone location.

The second phase is the system design phase. The requirement of the system specification from the first phase are studied. During this phase, the infrastructure of the interface is design based on the user requirement and the detailed analysis of the new system. The prototype of UI (User Interface) design, Use Case design and database design document in the Software Design Documentation. There is the prototype of UI design of this application:

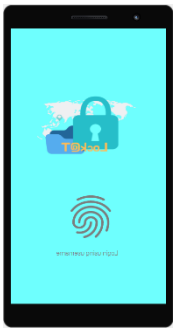

Figure 2: Fingerprint Login Page

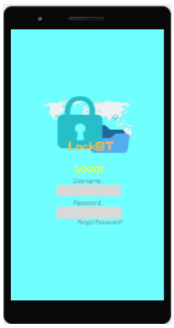

Figure 3: Username & Password Login

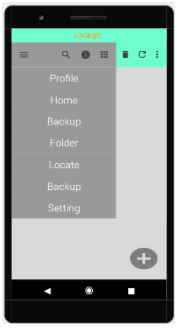

Figure 4: Profile Page

Figure 5: Folder Page

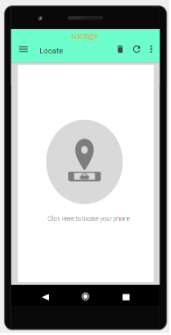

Figure 6: Location Page

The implementation & Coding phase is where the system will start to implement by producing the actual coding during this phase. This phase includes a task such as the UI development and implementation coding of the encryption technique.

Software Requirement of the system:

1. Operating System: Windows 10
2. Programming Language: JAVA/CSS/HTML
3. IDE: Visual Code, Apache Cordova, Ionic, SDK
4. Database: Firebase

Finally, the testing phase will proceed after the code is developed, it will be tested against the requirements. It will make sure the problem statement is solved based on the system requirement. To test the application the questionnaire is created and give to the 10 testers to differentiate between the previous application and this application to compare the result.

After the testing phase, if the application is satisfied then the process is development is finish. If the

system are not satisfied, the process will back to the first phase to recheck the system requirement.

Proposed System

In this era, the mobile phone had become a very important device for everyone. Many users think that it is safe and easier to store their confidential data on their phones. But with nowadays technology, the issue like spamming, hacking and cracking is getting worst. In the existing system, the AES algorithm used required user to insert different keys for different types of data for the encryption and decryption process which makes users need to remember many keys. This makes AES technique need longer time in processing. The proposed system is developed using the OTP (One Time Pad) cryptography technique, where a user only needs one password to encrypt and decrypt the data. The UI (User Interface) of the system will be more user-friendly for the user to easily understand the system. The system that will be developed with fingerprint authentication feature which allows only authorized user can access the system. The future improvement from the existing system, the proposed system will have a phone location tracker that allows a user to locate their phone if the phone is stolen or missing.

Expected Result and Discussion

Character	**Folder Lock**	**ZenCrypt**	**MyApp**
Authentication	Pin and fingerprint	Free: No Paid: Yes	Fingerprint and email and username
Encryption	NO	AES 128	OTP
Backup	Free: No Paid: Yes	No	Yes
Location Track	No	NO	Yes

Conclusion

Confidential and private data must be stored in a secure way that only can be seen and access by the authenticate user. Encryption technique is used to protect the data from malicious user. Security is the main purpose of this project that provides users to keep their data in a secured folder and only authorized users can retrieve the data. As the implementation of this system, this system provide user the location of their mobile device if the user loses their phone.

References

[1] 'What is Data Protection and Why is it Important? Definition from WhatIs.com', *SearchDataBackup*. [Online]. Available: https://searchdatabackup.techtarget.com/definition/data-protection. [Accessed: 18-Nov-2019].

[2] K. S. A. at law and Partner, 'Three reasons why we need strict data protection regulations', *NJORD Law Firm*, 09-Feb-2018.

[3] 'Number of mobile phone users worldwide 2015-2020', *Statista*. [Online]. Available: https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/. [Accessed: 18-Nov-2019].

[4] Ms. N.S. Gurdhalkar, Ms.P.D. Belhekar, Ms. J.S. Mane & Prof. T.R. Shinde. (January 2018). Mobile Self Encryption. International Journal of Advanced Research in Computer and Communication Engineering, Vol. 7, Issue 1.

[5] V. Jagtap, T. Ingale, V. Walke, S. Satpute, and A. S. Khandagale, 'Mobile Self Encryption System', vol. 8, no. 2, p. 4, 2019.

[6] Deebika.T, Dhanalakshmi.S , Durga.S , Francis Shamili.S, Merlyne Sandra Christina. (March 2016). Anti Theft Mobile Tracker Application. International Journal of Innovative Research in Computer, (pp. Vol. 4, Issue 3).

[7] LLC, N. (n.d.). Google Play. Retrieved from Folder Lock: https://play.google.com/store/apps/details?id=com.newsoftwares.folderlock_v1

[8] Zestas. (n.d.). Google Play. Retrieved from ZenCrypt - Securely Encrypt Files: https://play.google.com/store/apps/details?id=com.zestas.cryptmyfiles

[9] 'Agile Model & Methodology: Guide for Developers and Testers'. [Online]. Available: https://www.guru99.com/agile-scrum-extreme-testing.html. [Accessed: 18-Nov-2019].