EasyChair Preprint

№ 5817

# Password Vault

Shubhankar Vishwakarma, Heena Khera and
Kanishk Manchanda



June 16, 2021

# Password Vault

Shubhankar Vishwakarma
Computer Science And Engineering
Galgotias University
Greater Noida, India
shubhankar72380@gmail.com

Heena khera
(Assistant Professor)
Galgotias University
Greater Noida,India
heena@galgotiasuniversity.edu.in

Kanishk Manchanda
Computer Science And Engineering
Galgotias University
Greater Noida, India
kanishk131201@gmail.com

***As the increase in amount if users in social media the risk of getting their accounts and stealing their private information also increased and one of the way is to steal their password from the server which the person give permission to save in it while touching remember my password option.***

***Keywords—=Password Vault, Security, Password Breach, Password Leak***

## I. About Project

Password vault is actually nothing else then a password generating application. It is will help people to store their password at some cloud storage server which will be kept secure and also it will suggest some new strong password to the users as we all know password privacy is most important as due to password leakage many documents have got stolen by other people


Fig 1

Below is the graph for the leakage of the passwords and the lengths set by different lengths.

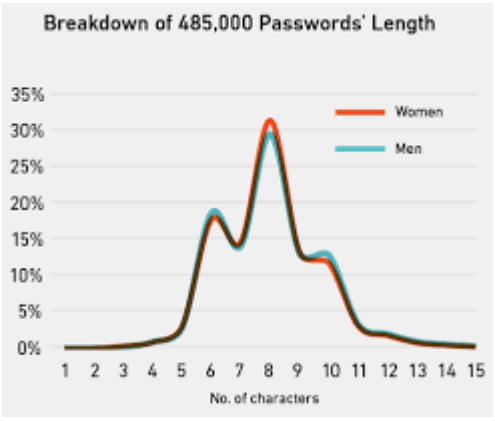


Fig 2

## II. Tooles Used

### *A. Android Studio:*

Since our application is a mobile application so the most useful tool to create is android studio which is mostly used for android application development. Most of the popular android applications are made by this software only. Below are its interface and logo.

Fig 3

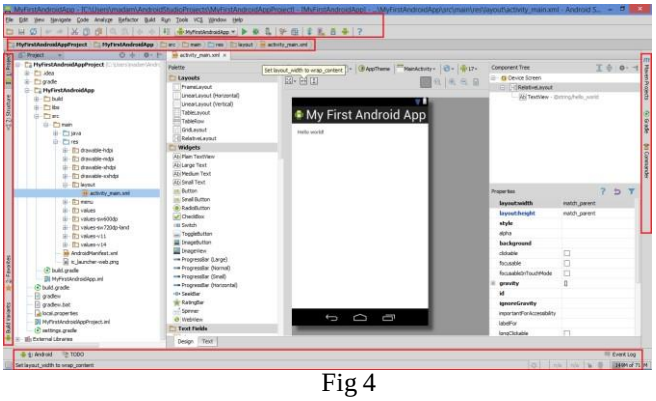


Fig 4

### *B. Firebase:*

Firebase is Google's mobile application development platform that helps us to improve, build and grow our application. We are using its real-time database feature to store the data of users like password and login credentials in a data base.

Fig 5

### *C. Miscelanious:*

Apart from Firebase and Android Studio we also require a computer machine on which we can work on with minimum 8 GB RAM, a stable internet connection, and Intel i5 processor, also an android device to run our application or

we can say to test our application on a physical device and to connect the physical device to the computer we also require a connection so for that data cable is used.

## III. LANGUAGES REQUIRED

Three languages are mainly required. (1) XML: Extensible Markup Language is used for designing the android application. (2) Data Base: To create data base of the credentials, data base is required. And lastly (3) Java/Kotlin: either java or Kotlin one out of both is required for back-end coding as a developer can choose accordingly which language is easy and suitable to him/her. Note: XML is required for front–end coding.

### A. *Abbreviations and Acronyms*

There are some Abbreviations which are used like Back-end, Front-end, API, Android Application, Data base and lastly Android which are important to understand. Because if we don't know them then we will confuse while developing the android application

### B. *API*

- Full form of API is Application Programming Interface. It is an intermediary that allows two applications to talk to each other
- We will be using HTTP and REST API in our application which will help in keeping users data secure.

### C. *Android*

Android is an Open Source Operating system used in mobile phones specially. This was developed Google and was released on 23 September 2008. Android Inc. was developed in Palo Alto, California, in October 2003 by Andy Rubin, Rich Miner, Nick Sears and Chris White. Presently there are 20 android versions present and we will be using android version 4.4 i.e. Kitkat and its API level is 19.

Android version 4.4 was first released on 31st October 2013.


Fig 6

We are this API level and android version because our app will be running 99.9% devices whose Android level is greater than or equal to 4.4 that is Kitkat android also most of the Android Applications easily runs on this version without any break down more over it is was also secure in that time with less bugs.

### D. *Data Base*

- The word ―data‖ is plural, not singular and are also known as raw facts and figures. Data Base is a collection of information which from which information can be accessed, managed and updated.
- We will be creating a data base, a real-time data base which is a feature of Google firebase to store the passwords of all the users

### E. *Front-End Development*

Front- End development is the user interface of an application by which users can interact to the applications and use it. The front end development consists of responsive buttons, images, pages, background, colors, designs, text used to display on the screen, font style etc. In fact for front end development of an android application we can do either by relative layout which is by xml files or we can also use constraint layout in which we can place the objects and items just by drag and drop method.

- We have used both relative and constraint layout for our application.

### F. *Back-End Development*

Back-End Development is the development which is done as the develop end. User don't have access to those codes and programming that's why only an APK file is shared whether by play stores or on internet. Back – End development consists of all the linking of pages and functioning of various options like delay of a page connecting a button to Gmail or opening of contacts are all part of none other than Back-End development. In our application we are using it for connection our application to firebase and connecting buttons to cloud server and password generator.

- The abbreviation ―i.e.‖ means ―that is‖, and the abbreviation ―etc.‖ means – Et cetera ‖.

### G. *Features Of Application*

Password vault Enterprise Functionality Master Password Reset Password vault Enterprise offers ―Super Admin‖ functionality, in which the enterprise can assign select administrators (deemed Super Admins) master password reset rights that provide them the ability to reset a user's master password. If Super Admins are assigned, when a new user is created or a master password is changed, a copy of the user's local key, used to encrypt and decrypt their vault, is encrypted to the Super Admin account. Only the Super Admin account can decrypt the local key to initiate a master password reset. Password vault does not allow Super Admins to access the contents of a user's vault via this functionality – only master password resets are permitted. . Vulnerability Management Internal and external system and network vulnerability scanning is conducted monthly. Dynamic and static application vulnerability testing, as well as penetration testing activities for targeted environments, are also performed periodically. These scanning and testing results

are reported into network monitoring tools and, where appropriate and predicated on the criticality of any identified vulnerabilities, remediation action is taken. Vulnerabilities are also communicated and managed with monthly and quarterly reports provided to the relevant development teams, as well as management. 3.10. Logging and Alerting LogMeIn collects identified anomalous or suspicious traffic into relevant security logs in applicable production systems.

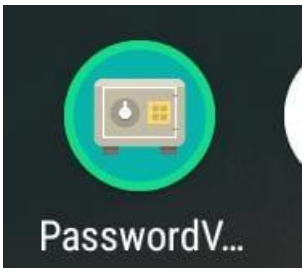


*Fig: icon of Android Application*

*H. Basic Design*

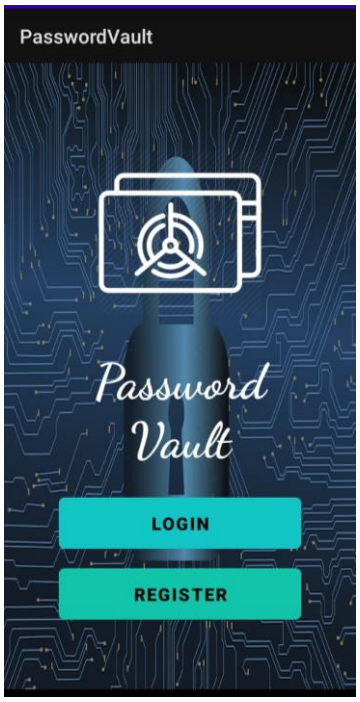


*Fig : Signup page- to choose whether to sign in or Register*


*Fig: Loin page to login the account this page will open on clicking on login buttion in fig1.*

*Fig: Splash screen very first screen and will go after few seconds*

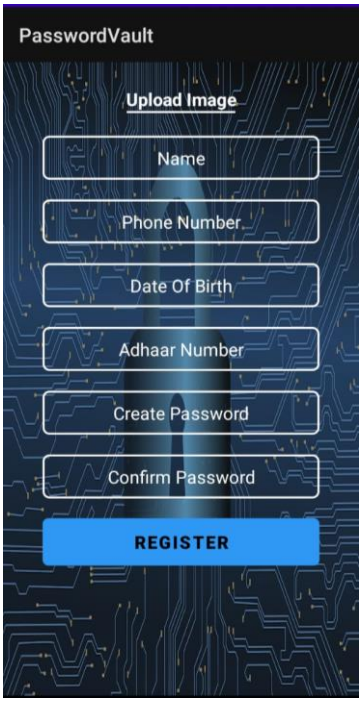


*Fig: to register on the application also called registration page.*

*I. Implementation*

The Passwordvault user is the only person that has full control over the encryption and decryption of their data. With Passwordvault, encryption and decryption occurs only on the user's device upon logging into the vault. Each individual record stored in the user's vault is encrypted with a random 256-bit AES key that is generated on the user's device. The record keys are protected by an additional key, called the Data Key. The Data Key is encrypted by a key derived on the device from the user's Master Password. Data stored at rest on the user's device is also encrypted by another key, called the Client Key. Secure record syncing between the user's devices is also encrypted at the network layer and routed through Passwordvault's Cloud Security VaultThis multi-tiered encryption model provides the most advanced data protection available in the industry. The encryption key that is needed to decrypt the data always resides with the Passwordvault user. KSI cannot decrypt the user's stored data.

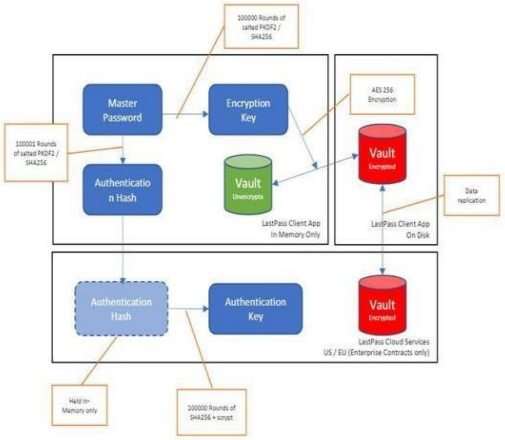


Fig 6

KSI does not have access to a customer's master password nor does KSI have access to the records stored within the Passwordvault vault. KSI cannot remotely access a customer's device nor can it decrypt the customer's vault. The only information that Passwordvault Security has access to is a user's email address, device type and subscription plan details (e.g. Passwordvault Unlimited). If a user's device is lost or stolen, KSI can assist in accessing encrypted backup files to restore the user's vault once the device is replaced. Information that is stored and accessed in Passwordvault is only accessible by the customer because it is instantly encrypted and decrypted on-the-fly on the device that is being used - even when using the Passwordvault Web App. The method of encryption that Passwordvault uses is a well-known, trusted algorithm called AES (Advanced Encryption Standard) with a 256-bit key length. Per the Committee on National Security Systems publication CNSSP-15, AES with 256-bit key-length is sufficiently secure to encrypt classified data up to TOP SECRET classification for the U.S. Government.

The cipher keys used to encrypt and decrypt customer records are not stored or transmitted to Passwordvault's Cloud Security Vault. However, to provide syncing abilities between multiple devices, an encrypted version of this cipher key is stored in the Cloud Security Vault and provided to the devices on a user's account upon successful vault login and multi-factor authentication. This encrypted cipher key can only be decrypted on the device for subsequent use as a data cipher key.

*J. Some More Infromation*

- Strong Master Password

It is highly recommended that customers choose a strong Master Password for their Password vault account. This Master Password should not be used anywhere outside of Password vault. Users should never share their Master Password with anyone.

- Two-Factor Authentication

To protect against unauthorized access to your vault, websites, and applications, Password vault also offers Two-Factor Authentication. Two-Factor authentication is an approach to authentication requiring two or more of the three authentication factors: a knowledge factor, a possession factor, and an inherence factor.

- Password vault uses something you know (your password) and something you have (the phone in your possession) to provide users extra security in the case where your master password or device is compromised. To do this, we generate TOTPs (Time- based One-Time Passwords).
- Password vault generates a 10-byte secret key using a cryptographically secure random number generator. This code is valid for about a minute, and is sent to the user by SMS, Duo Security, RSA SecurID, TOTP application, Google Authenticator or Password vault DNA-compatible wearable devices like the Apple Watch or Android Wear.

*K. Future Updates*

As we already know each and every good thing also have a drawback or we can also say disadvantages we already know some of it and we already started working on that also that what will be there in our future updates and below mentioned are some of them:

- The safety feature of the application will be enhanced and will be more secured since it is a trial version so there are no penetration tests.
- Secondly we are using a dummy data in Google firebase for a time being which will be replaced

by other cloud server. In fact our all system will move to a cloud server later on.

- Moreover this application will only be running on android devices but there are also some percent of population who cannot avail an android device or who cannot use an android device for them we will be also building a website through which they can remotely access their account.
- One last update will be their i.e. this application is only for android devices so it will only be available for android devices but what about Apple IOS users for them IOS based software will also be developed.

## ACKNOWLEDGMENT

We would like to say thank you to our Guide, our Mentor Ms. Heena Khera who guided us each and every step showed the way from starting till end and even helped in making this project named ―Password Vault‖ and a special thanks to our Dean Dr. Munish Sabharwal who gave us such a magnificent opportunity to show case out talent in doing this project. This project also helped is to improve our some of the skills yes we also learned some of the new things while making this application and also a thank you greeting to our parents, friends and our siblings who supported us indirectly as they didn't let our hope and enthusiasm to fall down.

## REFERENCES

This template has number citations consecutively within brackets [1]. The sentence punctuation follows the bracket [2]. Refer simply to the reference number, as in [3]—do not use ―Ref. [3]‖ or ―reference [3]‖ except at the beginning of a sentence: ―Reference [3] was the first ...‖

[1] YouTube channel of neetrootsTrans

[2] Head ahead with java 7 TH edition text book for some java langyage help

[3] Android Application Development All-in One For Dummies by Barry A. Burd

[4] K. Elissa, ―Android Tracking Device if known,‖ unpublished.

[5] R. Nicole, ―Android tracking device with only first word capitalized,‖ J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, ―Electron spectroscopy studies on magneto-optical media and plastic substrate interface,‖ IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

**End Of IEEE Conference template**