International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 06 | June - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

Password Tracker

Jagadish khatau
B.Tech
School of Engineering
Hyderabad, India
2111CS020181@mallareddyuniversity.ac.in

K.Sai Pavan Goud
B.Tech
School of Engineering
Hyderabad, India
2111CS020183@mallareddyuniversity.ac.in

P.Jahnavi
B.Tech
School of Engineering
Hyderabad, India
2111CS020185@mallareddyuniversity.ac.in

Jagadishwar Reddy
B.Tech
School of Engineering
Hyderabad, India
2111CS020182@mallareddyuniversity.ac.in

B.Vishnu Vardhan
B.Tech
School of Engineering
Hyderabad, India
2111CS020184@mallareddyuniversity.ac.in

M.Janaki
B.Tech
School of Engineering
Hyderabad, India
2111CS020186@mallareddyuniversity.ac.in

Guide: Sanjay Kumar J.H
Professor
School of Engineering,
Mallareddy University
sanjaykumar@mallareddyuniversity.ac.in

Abstract :-As the technology evolved, people had many accounts that needed a password for authentication. A password is required to access a particular account or information. However, the way they keep their account information expose them to vulnerable threats such as hacking if the password is not protected appropriately. Password Management Application (PMA) can help user manage and keep their password on different account securely. The design of the system is to offer a solution on managing multiple passwords. Password Management Application (PMA) also applied an Advance Encryption Standard (AES) algorithm for securing user's data that kept in the application. The AES is chosen based from the research and analysis that has been made. Agile framework is being used in completing this project. The Functionality Test technique has been applied to test the usability of the application. It has been done by a qualified tester and been approved to become the solution for user to use this application to recover their password management more efficiently. This application can help user manage and keep their password of different account securely. The limitation is where the application is only available for android application device. As for future recommendation, the Password Management Application should gives more access to social media or websites and different algorithm can be use on securing the password.

.

I. INTRODUCTION

People create their password according to something that related to them such as birth date, personal name, pet's name and phone number. Simple password especially a password that related to personal information is not recommended. Thisis because the simple password can easily be hacked by attacker for example by using brute force attack and if the password exposed to the attacker, the entire user's informationcan be stolen., the aim of this project is to develop an androidapplication that able to link users authenticate data directly toits account and also able to stored password information securely in the database. Information in the application stored in the database is secured by using an encryption method. Encryption is a process where data pass through a mathematical algorithm of encryption to encrypt a plain text to an unreadable text called cipher text and same process happento decrypt the data (Rayarikar, Upadhyay, & Pimpale, 2012). This method used to protect the information from unauthorizeduser or hacker to access such information.

II. PROBLEM STATEMENT

The objective of a password management application using encryption techniques is to securely store and manage sensitive user passwords and other confidential information. Encryption is a technique used to convert plain text into a code that cannot be easily read by unauthorized individuals. Password management applications typically use encryption to protect the user's data. When a user enters their password into the application, the password is encrypted using a strong encryption algorithm before being stored in the application's database. This ensures that if the database is ever compromised, the passwords will be unreadable to anyone who does not have the encryption key.

III. LITERATURE REVIEW

Password manager apps have gained significant popularity in recent years as individuals and organizations strive to enhance their digital security. This literature review examines the existing research and studies related to password manager apps. The review explores the benefits, limitations, and user experiences associated with these apps, as well as the underlying security considerations. Additionally, it highlights emerging trends and future directions in password manager app development and usage. The security considerations section delves into the encryption mechanisms, key management, and authentication protocols employed by password manager apps. It discusses the importance of end-to- end encryption, secure storage of passwords, and measures to prevent password leakage and unauthorized access. Python provides several libraries for implementing encryption algorithms, such as the PyCrypto and cryptography libraries. These libraries can be used to implement

strong encryption algorithms such as AES in the password management application. AES encryption function is used to encrypt the information that need to be secured. It happens in a background process during the saving of new memo created by user. Cipher class provides access to implementation of cryptographic ciphers for encryption and decryption. Once getInstance method is called, the data will be encrypted to base 64 format by using AES algorithm.Django provides built-in support for multi-factor authentication using the Django Two-Factor Authentication library. This library provides methods for implementing TOTP and other multi-factor authentication methods.: Django provides built-in support for database backup and recovery using the Django Backup and Django DB Backup libraries. In conclusion, Python and Django provide a robust platform for developing a password management application using encryption techniques. These technologies can be used to implement strong encryption algorithms, generate random passwords, provide multi-factor authentication, and create an intuitive user interface.

IV. REQUIRED TOOLS

- Django
- Jupyter
- Python
- SQLite
- Libraries like Encryption ,User Interface etc..

V. METHODOLOGY

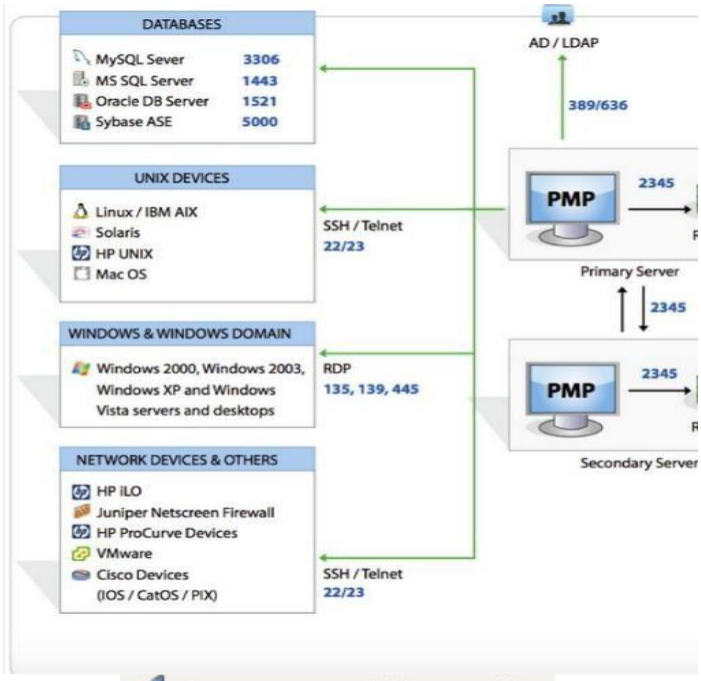
Cryptography is the science to encrypt and decrypt data that enables the user to store sensitive information or transmit it across insecure networks so that it can be read only by the intended recipient. There are two kinds of encoding. Those two types are the symmetric and asymmetric encoding algorithms. Several of those algorithms will be included hereinsuch as: AES, DES etc.

Fig:-Methodology

.

VI. EXPERIMENT RESULTS

Fig:-entering the master password to go for further steps To enter account name, user name, password



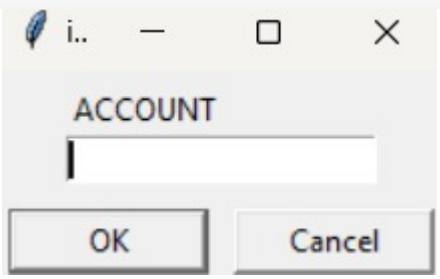


Fig:-To enter account name

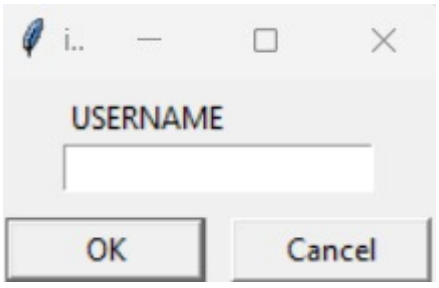


Fig:- To enter user name

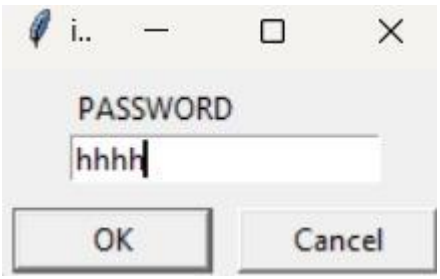


Fig:-To enter password

Fig:-To store all the passwords

VII. ARCHITECTURE DIAGRAM FOR PROPOSED METHOD

Fig: System Architecture

VIII. CONCLUSION:

As the technology evolved, people had many accounts that needed a password for authentication. A password is required to access a particular account or information. However, the way they keep their account information expose them to vulnerable threats such as hacking if the password is not protected appropriately. Password Management Application (PMA) can help user manage and keep their password on different account securely. The design of the system is to offer a solution on managing multiple passwords. Password Management Application (PMA) also applied an Advance Encryption Standard (AES) algorithm for securing user's data that kept in the application. The AES is chosen based from the research and analysis that has been made. Agile framework is being used in completing this project. The limitation is where the application is only available for android application device. As for future recommendation, the Password Management Application should gives more access to social media or websites and different algorithm As the technology evolved, people had many accounts that needed a password for authentication. A password is required to access a particular account or information. However, the way they keep their account information expose them to vulnerable threats such as hacking if the password is not protected appropriately. Password Management Application (PMA) can help user manage and keep their password on different account securely

IX. Future Enhancement:

In future, several modifications can be done in this project like:

- Enhancing the user interface to make it more interactive to users.

- A more enhanced login panel with more security measure to deal with cyber-attacks properly.

• We will be hosting this tool on a website and enhancing our database to manage a greater number of user entries

ACKNOWLEDGEMENT

We would like to thank Dr.VSK Reddy, Vice Chancellor, MRUH, Hyderabad for providing an excellent academic environment in the college and her never-ending support for the program. We would like to express our gratitude towards Dr. Thayyaba Khatoon, Professor and HOD, Department of Artificial Intelligence & Machine Learning, MRUH, Hyderabad, who provided guidance and gave valuable suggestions regarding the project. We consider it a privilege and honour to express our sincere gratitude to our internal guide Sanjaykumar J. H , Asst. Professor, Department of Artificial Intelligence & Machine Learning, , MRUH , Hyderabad, for his valuable guidance throughout the tenure of this project work. We would like to thank all the faculty members who have always been very cooperative and generous. Conclusively, we also thank all the nonteaching staff and all others who have done immense help directly or indirectly during our project

REFERENCES

[1] Theory Segment: ChatGPT
[2] Images: google chrome
[3] Architecture: https://www.google.com/imgres
[4] https://projectsgeek.com/2017/12/password- management-system-project.html