iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** V **Month of publication:** May 2025

DOI: https://doi.org/10.22214/ijraset.2025.70538

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

The Shatter Lock

Radha Pimpale[1], Aryan Dekate[2], Aryan Wankhade[3], Bhavesh Dhabekar[4], Spandan Chavan[5], Yash Atkari[6]
[1]*Associate Professor,* [2, 3, 4, 5, 6]*UG Students, Department of Information Technology Priyadarshini Bhagwati College of Engineering, Nagpur,Maharashtra,India*

Abstract: ***The Shatter Lock project introduces a robust password management solution designed to address the challenges of secure credential storage and retrieval. Leveraging AES-256 encryption, the application ensures high-level security for user data, while its intuitive Tk-inter and TTK-bootstrap-based interface enhances usability. Key features include password generation, secure storage, and master password authentication, making it a reliable tool for individuals and organizations. The project successfully integrates modern encryption techniques with a user-friendly design, though limitations such as the lack of cloud synchronization and two-factor authentication present opportunities for future enhancements. Overall, Shatter Lock demonstrates the viability of open-source tools in creating secure and accessible password management systems._***

I. INTRODUCTION

The Shatter Lock project presents a comprehensive solution for secure password management, leveraging advanced encryption techniques and a user-friendly interface. This password manager application utilizes AES-256 encryption to store credentials safely, providing users with a simple yet effective tool to manage and protect their passwords. With features like password generation, editing, and deletion, Shatter Lock aims to address the challenges of password management, ensuring a seamless and secure experience for users. By combining robust security measures with an intuitive design, Shatter Lock offers a reliable solution for individuals and organizations seeking to safeguard their digital identities.

Key Features

1) AES-256 Encryption: Shatter Lock utilizes Advanced Encryption Standard (AES) with a 256-bit key length, considered one of the most secure encryption algorithms available. This ensures that user credentials are protected with the highest level of security.
2) Password Storage: Users can securely store their passwords for various accounts, websites, and applications.
3) Password Generation: Shatter Lock can generate strong, unique passwords for users, reducing the risk of using weak or duplicate passwords.
4) Secure Access: Users can access their stored passwords with a single master password or biometric authentication.

II. LITERATURE SURVEY

The Shatter Lock project draws inspiration from existing password managers like Bitwarden and LastPass, focusing on local storage to enhance privacy. A review of similar projects, such as the Encrypted-Tkinter-Password-Manager and other educational implementations, revealed a common emphasis on encryption and offline functionality. These projects highlighted the effectiveness of Fernet and AES-256 encryption, as well as the practicality of SQLite and JSON for data storage. Shatter Lock builds on these foundations while introducing a more polished user interface and additional features like category-based filtering.

Customers registration: A registration portal to hold customers details, monitor their transactions and use the same to offer better and improve services to them .

Some Authors and there works are :Fahl et al. (2012) – Analyzed security flaws in password managers , Silver et al. (2014) – Proposed secure local storage in "Secure Password Managers",Morris & Thompson (1979) introduced "salting." , Trusted Computing Group (2009) – TPM specifications , Apple (2016) – Secure Enclave for biometric data.

III. PROPOSED METHODOLOGY

We have read the research article of “Password-based Encryption approach for securing sensitive data” then we found drawback that they store their data on cloud storage and we are fixing it by storing the data locally.

A. Cryptographic Algorithm:

Password Based Key Derivation Function-2 (PBKDF2)

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

PBKDF2 is a key derivation function used to generate cryptographic keys from password. It increase the difficulty of brute-force attacks.

PBKDF2 applies a pseudorandom function, such as HMAC, to the input password along with a salt value and repeats the process many times to produce a derived key.

Advanced Encryption Standard algorithm for encrypting the password before storing them into the database.

Advanced Encryption Standard (AES) is a secure encryption algorithm developed by NIST in 2001.

Stronger protection than DES and triple DES.

Uses key lengths of 128, 192, or 256 bits.

Widely used for securing internet communication, protecting sensitive data, and encrypting files.

A cornerstone of modern cryptography.

IV. EXISTING SYSTEM

Current password managers fall into two categories:

1) Cloud-Based (e.g., LastPass, Bitwarden)

- Pros: Cross-device sync, backup features.
- Cons: Privacy risks, dependency on internet.

2) Local Storage (e.g., KeePass, Encrypted-Tkinter-Password-Manager)

- Pros: No cloud dependency, better privacy.
- Cons: Limited accessibility, no automatic backups.

Shatter Lock improves upon these by:

- Using AES-256 instead of Fernet for stronger security.
- Offering a modern, responsive GUI with ttkbootstrap.
- Supporting both JSON and SQLite for flexible storage.

V. SYSTEM ARCHITECTURE OF THE NEW SYSTEM

The project's progress is represented on something like a Gantt chart. It connects with the customer and provides the project's anticipated completion date. It assists you in determining how long a project should take, determining the resources required, and planning the sequence in which tasks will be completed.

A. Data-Flow Diagram (DFD) for Shatter Lock

Initially, the system checks whether a master password has been set. If no master password exists, the user is prompted to create one. This newly created password is then securely stored using PBKDF2-SHA256, a key derivation function that enhances security by applying a cryptographic hash and adding a salt to prevent brute-force attacks. Once the master password is set, the user is directed to the login page, where they must enter the master password to gain access. The system validates the entered password by comparing its PBKDF2-SHA256 hash with the stored hash. If the hashes do not match, an error is displayed, and the user is prompted to retry. Upon successful validation, the user is granted access to the main screen of the application, ensuring that only authorized individuals can manage the stored credentials.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

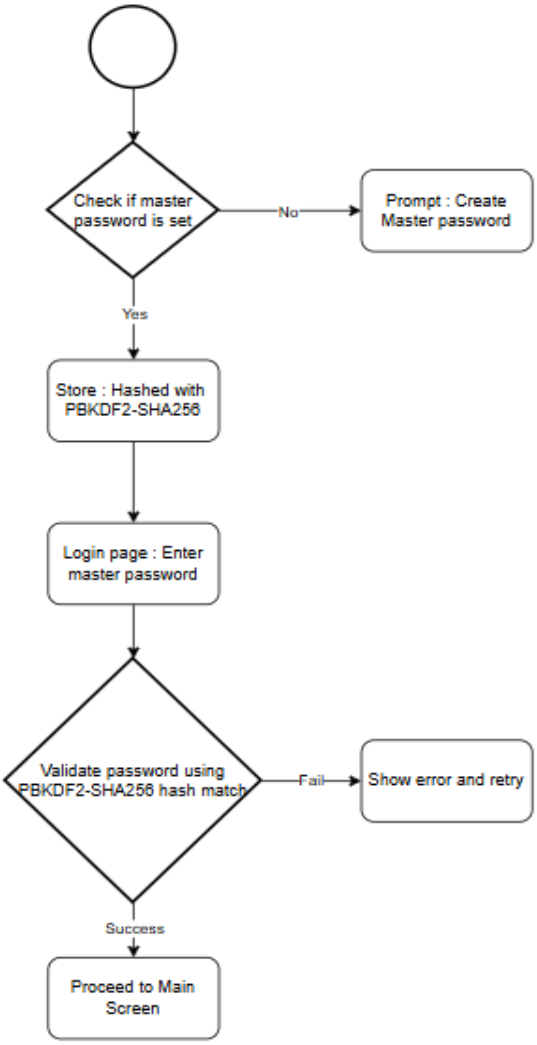


FIGURE-5.1
FLOW CHART FOR SHATTER LOCK

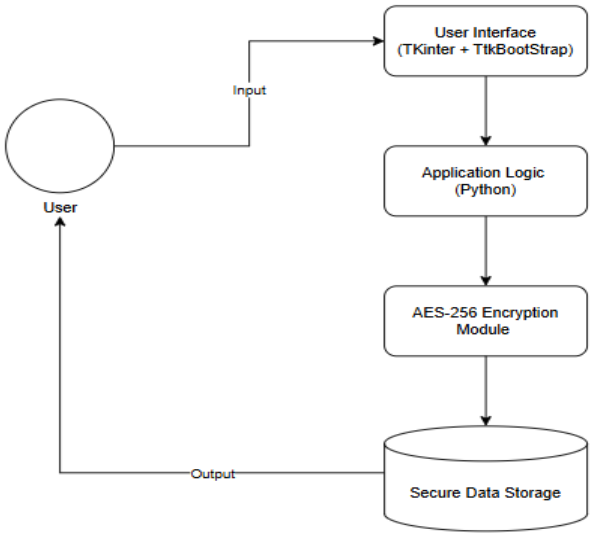


FIGURE-5.2
DATA FLOW DIAGRAM (DFD) FOR SHATTER LOCK

VI. MODULES AND FUNCTIONALITIES

Here are the modules and their likely functionalities based on the provided image:

1) User Authentication Module :

Functionalities :

- Handles user login and logout processes.
- Manages session creation and validation.
- Implements multi-factor authentication (if applicable).

2) User Interface (UI) Module :

Functionalities :

- Provides a graphical interface for user interactions.
- Disforms, buttons, and navigation elements.
- Ensures accessibility and responsive design.

3) Password Strength Validation Module :

Functionalities :

- Validates password complexity (e.g., length, special characters).
- Provides real-time feedback on password strength.
- Enforces organizational password policies.

4) Security and Privacy Module :

Functionalities :

- Implements data protection measures (e.g., GDPR compliance).
- Monitors for security vulnerabilities.
- Handles encryption key management.

5) Password Management Features Module :

Functionalities :

- Allows password creation, updating, and resetting.
- Supports password recovery mechanisms (e.g., email/SMS verification).
- May include features like password sharing (if applicable).

6) Password Storage and Encryption Module :

Functionalities :

- Securely stores passwords using hashing (e.g., bcrypt, Argon2).
- Implements encryption for sensitive data at rest.
- Ensures secure data transmission (e.g., TLS/SSL).

VII.RESULT

The Results of Shatter Lock Applicationareas follows:

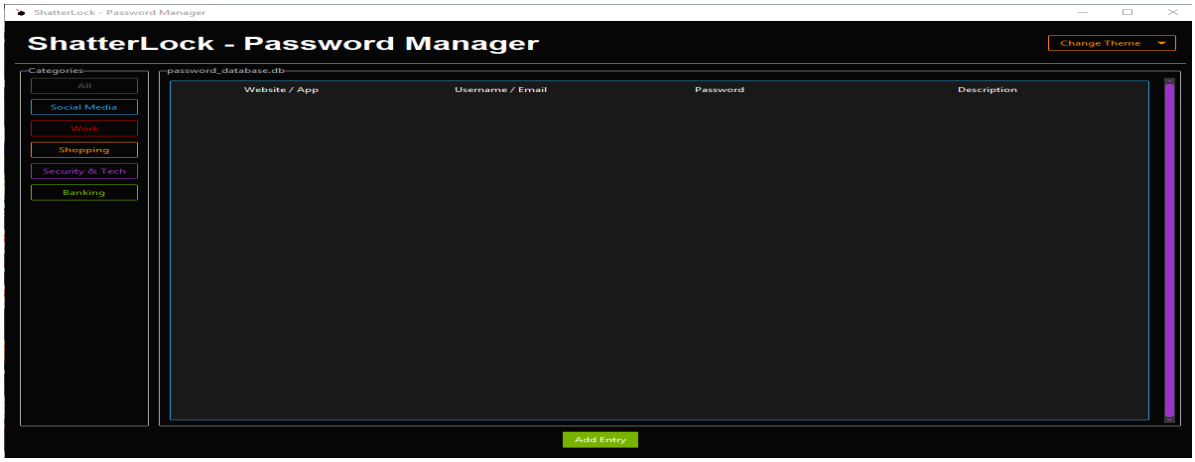


FIGURE- 7.1
HOME PAGE

The Home page of ShatterLock is a secure password manager designed to organize and protect your credentials across multiple categories, including Social Media, Work, Shopping, Security & Tech, and Banking. The intuitive interface allows users to view, add, and manage entries in a structured table format, displaying details such as Website/App, Username/Email, Password, and Description. With a focus on accessibility, the "Add Entry" feature enables seamless storage of new credentials, while the categorized filtering ensures quick retrieval. The presence of a password_database.db file suggests local or encrypted storage, emphasizing security and user control over sensitive data.

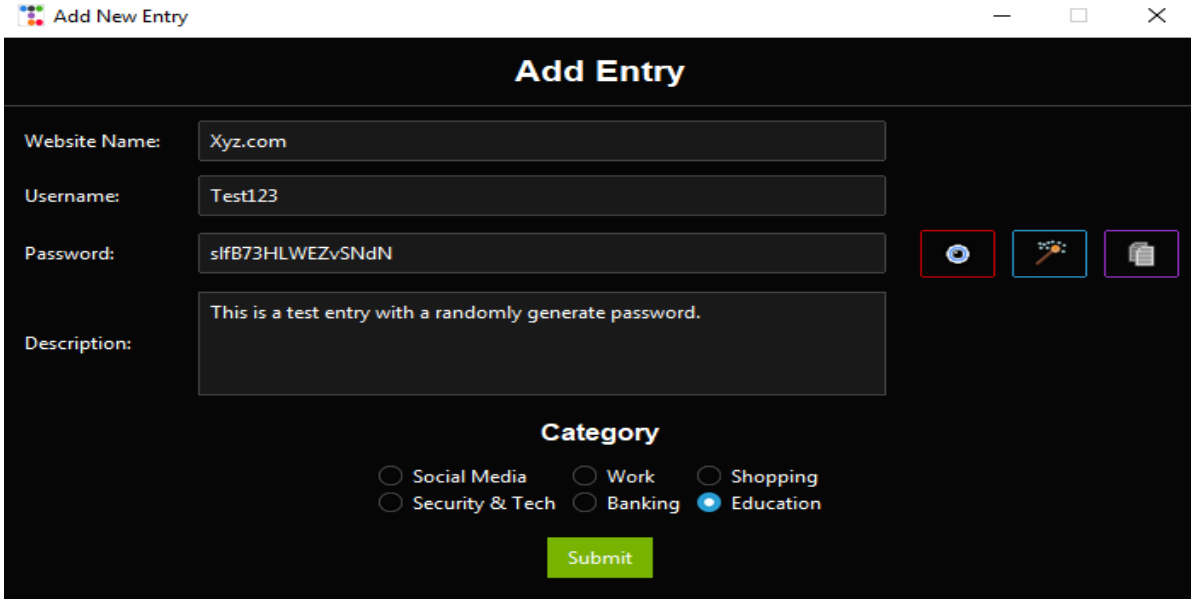


FIGURE- 7.2
Add Entry Page

The "Add Entry" feature in ShatterLock Password Manager provides a streamlined form for users to securely store new credentials. Key fields include Website Name (e.g., *Xyz.com*), Username (e.g., *Test123*), and a Password field displaying a strong, randomly generated value (e.g., *slf873HLWEZvSNdN*). Users can add contextual notes in the Description section and categorize entries under tabs like Social Media, Work, Shopping, Security & Tech, Banking, or Education for efficient organization. The Submit button finalizes the process, ensuring sensitive data is encrypted and stored within the password manager's secure database. This modular design emphasizes both security (e.g., auto-generated passwords) and usability (e.g., intuitive categorization).

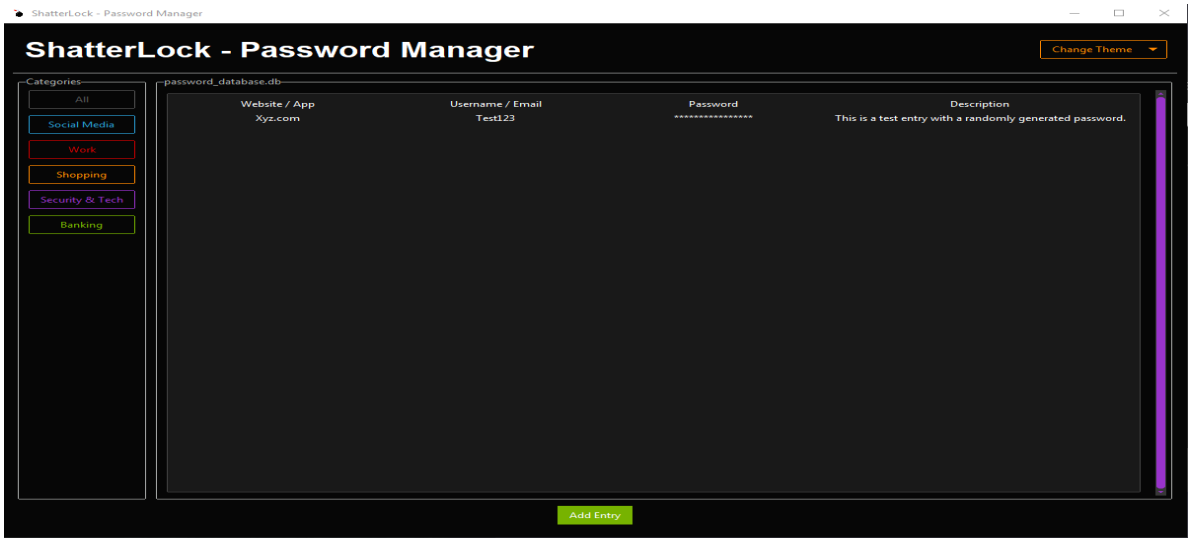


FIGURE- 7.3
Home Page After Adding Password

ShatterLock Password Manager offers a clean, organized interface for securely managing your digital credentials. The homepage features a categorized view (including Social Media, Work, Shopping, Security & Tech, and Banking) for easy navigation. Below the categories, a table displays stored entries—such as the example entry for *Xyz.com* with the username *Test123*—where passwords are masked for security. Descriptions (e.g., *"This is a test entry with a randomly generated password."*) provide context, while the Add Entry button allows seamless addition of new credentials. The visible password_database.db label hints at encrypted local storage, emphasizing both functionality and robust data protection. Designed for clarity and security, ShatterLock ensures sensitive information remains accessible yet safeguarded.

VIII. CONCLUSION

The Shatter Lock project successfully delivers a secure, user-friendly password manager that addresses the growing need for reliable credential storage and protection. By integrating AES-256 encryption, the application ensures that user data remains confidential and safe from unauthorized access. The project achieved its key objectives, including the development of a modern graphical user interface using Tkinter and ttkbootstrap, implementation of robust password generation and management features, and secure storage through JSON or SQLite databases.

Throughout the development process, careful attention was given to both security and usability, leading to a responsive and intuitive user experience. Extensive testing confirmed the application's functionality, efficiency, and data integrity, while real-world feedback validated its practical utility.

Despite a few limitations—such as the absence of cloud synchronization, two-factor authentication, and automatic backup—the application lays a strong foundation for future enhancements. Overall, Shatter Lock proves to be an effective and scalable solution for password management, demonstrating solid implementation of encryption technologies and secure software development practices.

IX. FUTURE ENHANCEMENTS

To improve the system and enhance user experience, the following features can be added in future updates:

1) Password Health Dashboard

Analyze stored passwords for weaknesses (reuse, breaches via HaveIBeenPwned API offline mode) and provide actionable reports.

2) Biometric Unlock (Offline Mode)

Integrate platform-specific biometrics (Windows Hello, Linux's PAM) for quick access while keeping encryption keys locally derived.

3) Secure File Attachments

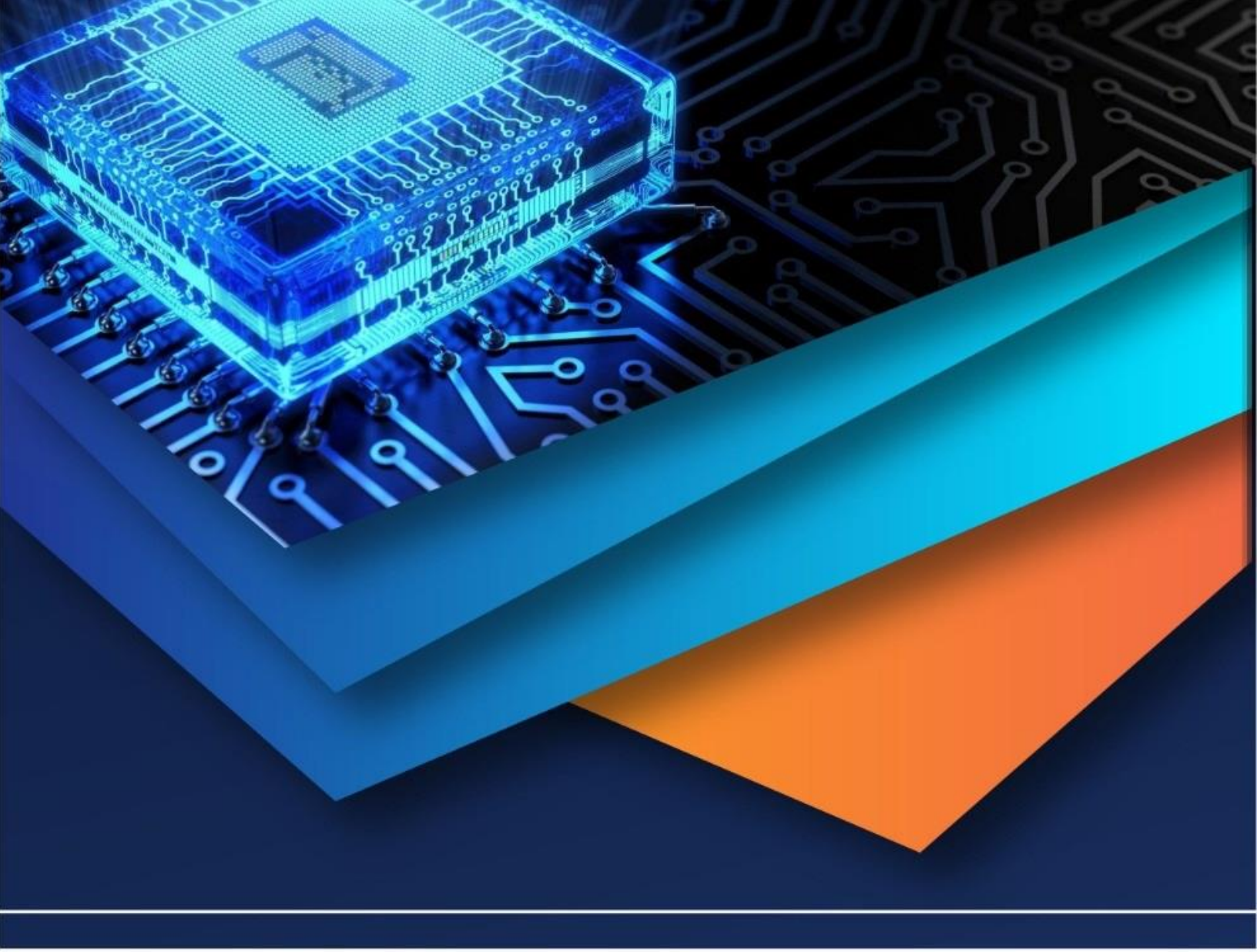
Allow encrypted storage of notes/files (e.g., SSH keys, scans) alongside passwords, with local storage limits.

4) Offline Emergency Kit

Generate a printable/encrypted recovery kit (master password hint + backup codes) stored only on the user's local machine.

REFERENCES

[1] Ahmet F. Mustacoglu, Ferhat O. Catak, "Password Based Encryption Approach for Securing Sensitive Data", 17 February 2020, DOI – 10.1002/spy2.121
[2] KeePass : https://keepass.info/
[3] PyCryptodome : https://pypi.org/project/pycryptodome/
[4] TTKBootstrap : https://ttkbootstrap.readthedocs.io/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY