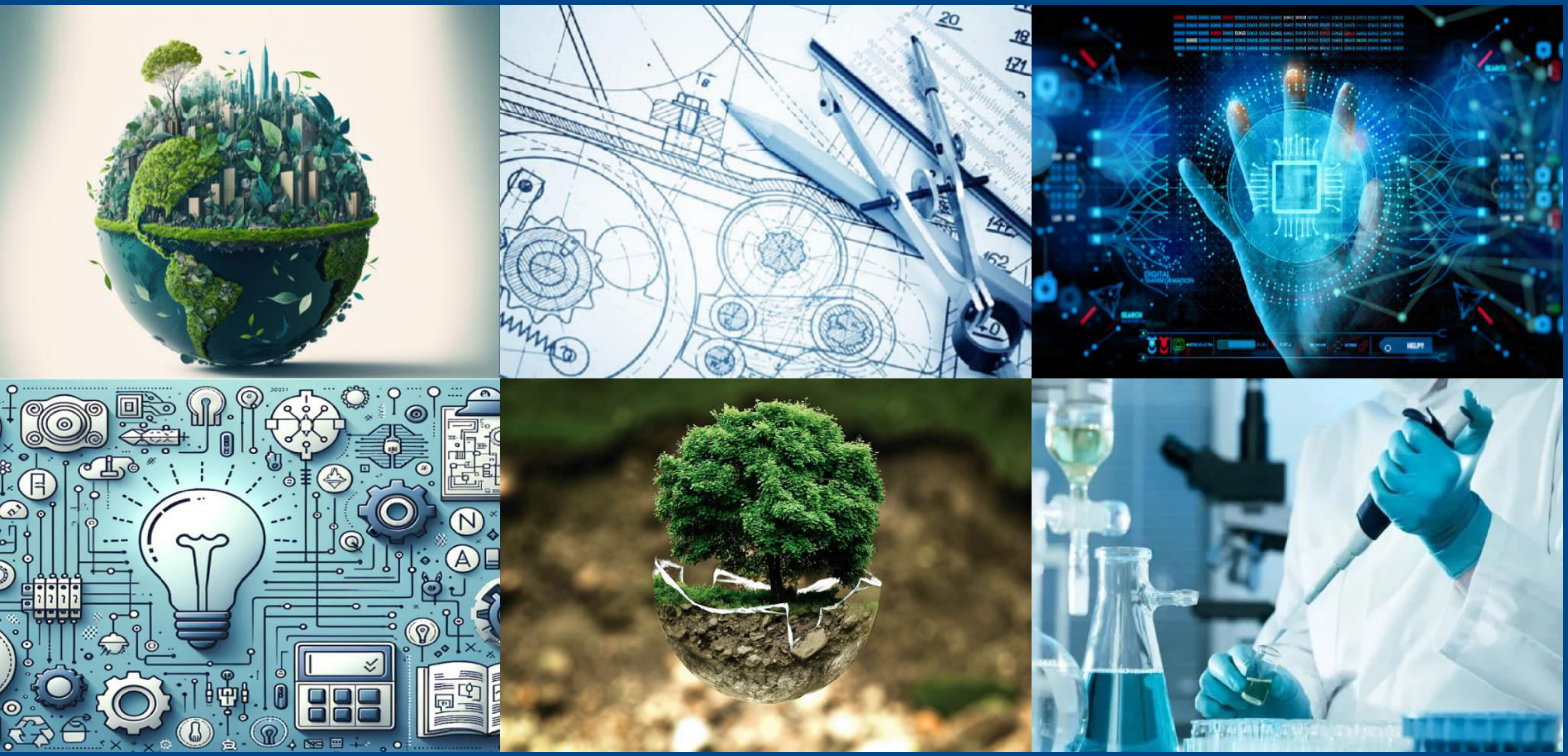
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 6, June 2025

ISSN: 2582-7219 |www.ijmrset.com |Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Encrpytopass: Password Storage and Retrieval System and Retrieval System with Breach and Security Notifications

D. Prabhakaran, Dr. T. Geetha, V. Monisha

Assistant Professor, Department of Master of Computer Applications, Gnanamani College of Technology(Autonomous), Namakkal, Tamil Nadu, India

HOD, Department of Master of Computer Applications, Gnanamani College of Technology (Autonomous), Namakkal, Tamil Nadu, India

PG Student, Department of Master of Computer Applications, Gnanamani College of Technology (Autonomous), Namakkal, Tamil Nadu, India

ABSTRACT: Every day, the number of traffic accidents rises as the automobile population increases. According to a survey by the **World Health Organization (WHO),** 1.3 million people die and 50 million are wounded annually around the globe. Most people die because they don't get medical help at the scene of an accident or because it takes too long for rescuers to get there. The time after an accident can be optimally used to make a difference between a life saved and life lost, if recovery actions are able to take place in time.

However, routing problems and traffic congestion is one of the major factors hampering speedy assistance. By identifying sites where the possibility of accidents is higher and the closest spot for ambulance placement, the response time can be greatly reduced. In order to operate efficiently as well as effectively ambulances should be deployed in areas where there is maximum demand and the ambulance should be able to reach the victim within a drive time of five minutes.
.

I. INTRODUCTION

Passwords are crucial for digital security because they serve as the primary method of verifying a user's identity and granting access to protected systems or accounts. They act as the first line of defense against unauthorized access to sensitive information and digital assets, preventing malicious actors from gaining unrestricted entry. In the process

of authentication, users provide credentials—typically a username and password—to prove their identity to a system. This simple mechanism helps protect online accounts, devices, and files from unauthorized access by cybercriminals and malicious software, as highlighted by Microsoft.

II. SCOPE OF THE PROJECT

The Secure Password Managing System is designed to provide users with a safe and efficient way to manage their digital credentials. The system focuses on securely storing passwords using AES-256 encryption, ensuring confidentiality and protection against unauthorized access. It supports master authentication methods, including password and biometric options, to strengthen security during login. To further enhance account protection, the system incorporates two-factor authentication (2FA), reducing the risk of unauthorized access. It includes breach detection features that notify users about weak, reused, or compromised passwords, encouraging proactive security practices.

III. HARDWARE REQUIREMENTS

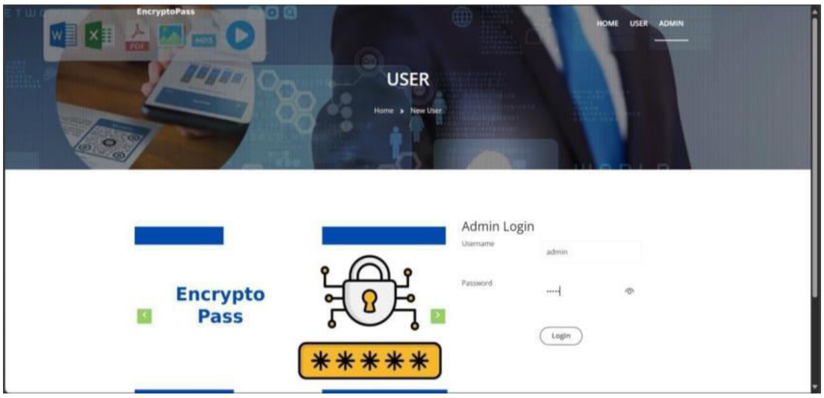
- **Processor** : Intel Xeon or AMD Ryzen series processor
- **RAM** :Minimum 16GB RAM, recommended32GB orhigherforbetter performance

- **Storage** : SSD storage for faster data access
- **Network** : Gigabit Ethernet for network connectivity

IV. SOFTWARE REQUIREMENTS

- **Operating System:** Windows, Linux, or macOS for server and client devices.
- **Backend Framework:** Python with Flask (or any preferred backend framework) for server-side logic.
- **Database:** MySQL or PostgreSQL for secure password storage.
- **Encryption Library:** AES-256 encryption library (e.g., PyCryptodome for Python).
- **Authentication Tools:** OTP generation and delivery service (via email/SMS API).
- **Frontend Technologies:** HTML, CSS, JavaScript, and Bootstrap for responsive user interface.
- **Web Server:** Apache or Nginx for hosting the web app.
- **Security Tools:** SSL/TLS certificates for secure communication (HTTPS).

V. METHODOLOGY



Admin Login

Username admin

Password ····

1. Password Locker Dashboard

This is the main control panel of the system where users interact with their saved passwords. It offers a secure and organized environment, allowing users to easily add new passwords, modify existing ones, or remove those they no longer need. The dashboard is designed to help users categorize their passwords, which makes finding and managing them simpler. Importantly, it also acts as a security assistant by alerting users instantly if any password is weak, has been reused, or is found in known data breaches. These alerts encourage users to improve their password strength and overall account security.

2. End User (Admin, User)

The system distinguishes between two types of users, each with different access privileges to maintain security and proper management.

3. Authentication

The authentication module is the first and foremost line of defense in the system, ensuring that access to sensitive password data is granted only to verified and legitimate users. It begins with the conventional method of verifying user identity through username and password credentials. To bolster this security, the system employs Multi-Factor Authentication (MFA), which requires users to provide an additional verification factor—typically a One-Time Password (OTP) sent via email or SMS to the user's registered contact information.

4. Key Generation

This module plays a critical role in securing user passwords by creating strong, unique encryption keys that are essential for protecting sensitive data. Each password or password file is encrypted with a newly generated AES

(Advanced Encryption Standard) key, which is a highly secure and widely trusted symmetric encryption algorithm. The randomness and uniqueness of each key ensure that even if one encryption key is compromised, it does not jeopardize the security of other users' data. The module also includes a secure key management mechanism that safely stores these keys within the system and securely transmits them during encryption and decryption processes.

5. Password Decryption

This module is essential for allowing users to retrieve and view their original passwords securely when necessary. It performs the process of decrypting the encrypted password data stored in the database back into plain text. Using the specific decryption keys generated and managed by the Key Generation module, the Password Decryption module ensures that only authorized users—whose identity has been verified through the authentication system—can access the decrypted passwords. This strict authorization check prevents any unauthorized attempts to read sensitive data. The decryption process is designed to be highly secure, maintaining confidentiality and ensuring that passwords.

VI. CONCLUSION

In conclusion, this project successfully implements a secure and user-friendly Password Locker system designed to manage and protect users' sensitive credentials efficiently. By integrating robust encryption techniques, multi-factor authentication, and real-time breach alerts, the system ensures high levels of data confidentiality and security. The user-centric design facilitates easy password storage, retrieval, and management while preventing common security risks such as password reuse and unauthorized access. Additionally, comprehensive security measures, including secure communication protocols and thorough input validation, safeguard the system against cyber threats. While the current implementation effectively addresses password management challenges, future enhancements could focus on integrating biometric authentication, advanced anomaly detection, and cloud synchronization for seamless access across devices. Overall, this project significantly enhances password security and user convenience, contributing to safer digital identity management in an increasingly connected world.

REFERENCES

1. "Python Crash Course" by Eric Matthes – Comprehensive guide for Python programming.
2. "Flask Web Development" by Miguel Grinberg – Essential resource for learning Flask.
3. "Learning MySQL" by Russell J.T. Dyer – Beginner-friendly book for MySQL database management.
4. "Python for Data Analysis" by Wes McKinney – In-depth coverage of data analysis with Pandas.
5. "Python Data Science Handbook" by Jake VanderPlas – Excellent reference for NumPy, Matplotlib, and data science tools.
6. "Bootstrap 4 Quick Start" by Jacob Lett – Quick introduction to Bootstrap for responsive web design.
7. "Programming with WAMP" by Michael Pewtherer (online resources) – Useful reference for using WampServer in web development environments.

INTERNATIONAL JOURNAL OF
MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com