IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

CRYPTOSHIELD: PASSWORD GENERATOR AND LOCKER USING CRYPTOGRAPHY

[1]Anshika Dixit, [2]Ahsan Ahmad Siddiqui, [3]Dr Ashish Baiswar

[1]UG student of the Department of Information Technology, Shri Ramswaroop Memorial College of Engineering and Management Lucknow, Uttar Pradesh, India
[2]UG student of the Department of Information Technology, Shri Ramswaroop Memorial College of Engineering and Management Lucknow, Uttar Pradesh, India.
[3]Associate Professor, Department of Bachelor of Information Technology, SRMCEM, Lucknow, India

Abstract - In today's digital era, secure management of passwords is uppermost to shielding sensitive information. The stronger the password, the safer your data and devices will be from data breaches and thefts. We've often heard that the passwords for our online accounts should be really strong and also avoid using the same password everywhere, especially for those important accounts. And here comes the most common problem "Creating and remembering different passwords of different platforms " is hard. This project presents a clever way to deal with secret key administration and utilize cryptography and a modern application development framework. Employing symmetric algorithms for password generation, users are also relieved from the burden of memorizing complex passwords. Access is facilitated through a one-time password (OTP), enhancing both convenience and security. The app is developed on the Flutter platform and uses Firebase as a backend database, ensuring robust data storage and synchronization capabilities. With "Crypto-shield" the user doesn't need to worry about creating strong passwords and their storage.

Key Words: Password Manager, Password Generator, Cryptography, Encryption

INTRODUCTION

In our undeniably digitalized world, people use a large number of applications, and services on different devices which may also contain critical information. Digital data is equally important as gold for people these days which needs to be safe from intruders, this is where passwords come as a savior. Overseeing passwords has turned into a basic part of day-to-day existence. Each record requires areas of strength for a secret word to defeat unapproved access and safeguard delicate individual data.

However, the very next problem that arises here is creating and storing strong and unique passwords. It has been observed that a large number of people reuse their passwords and this increases the chances of unauthorized access. According to scientists, the human brain can store the equivalent of 2.5 million gigabytes of digital memory and is also creative still, we cannot deny the forgetful nature of humans. This problem can be easily tackled using crypto-shield this creative apparatus uses progressed cryptography strategies to produce strong, extraordinary passwords for each record, freeing clients from the weight of remembrance.

PROPOSED SYSTEM

The proposed framework for the Secret Word Generator and Storage project addresses a refined combination of state-of-the-art cryptographic strategies with natural client-driven plan standards, expecting to raise the principles of the secret phrase of the executives in the present computerized scene. At the core of this system lies the utilization of a symmetric algorithm for password generation, ensuring the creation of strong, unique passwords while obviating the necessity for users to memorize intricate passphrase combinations. Instead, the system implements a seamless authentication mechanism whereby users receive a one-time

password (OTP) via their registered phone number or email. This OTP serves as a robust means of verifying the user's identity, granting access to their stored passwords securely within the application.

Its commitment to user-friendliness and convenience is central to the system's design philosophy. Through a meticulously crafted user interface, the application offers an intuitive and visually appealing experience, allowing users to effortlessly manage their passwords with ease. Whether it's creating new passwords, deleting outdated ones, or updating existing credentials, the interface provides clear and accessible options, empowering users to maintain their digital security without the encumbrance of cumbersome processes.

Developed using Flutter, the application ensures cross-platform compatibility, enabling users to access their passwords seamlessly across a multitude of devices and operating systems. Using Firebase as the backend database further enhances the system's capabilities, offering scalability, reliability, and real-time data synchronization. This integration enables users to enjoy the convenience of instant access to their passwords while ensuring that their data remains securely stored and accessible whenever needed.

The proposed system represents a holistic approach to password management, seamlessly blending robust encryption techniques, secure authentication protocols, and user-centric design principles. By prioritizing both security and usability, the system endeavors to redefine the user experience associated with password management, offering a secure, convenient, and accessible solution for individuals navigating the complexities of digital security in the modern age.

WORKFLOW

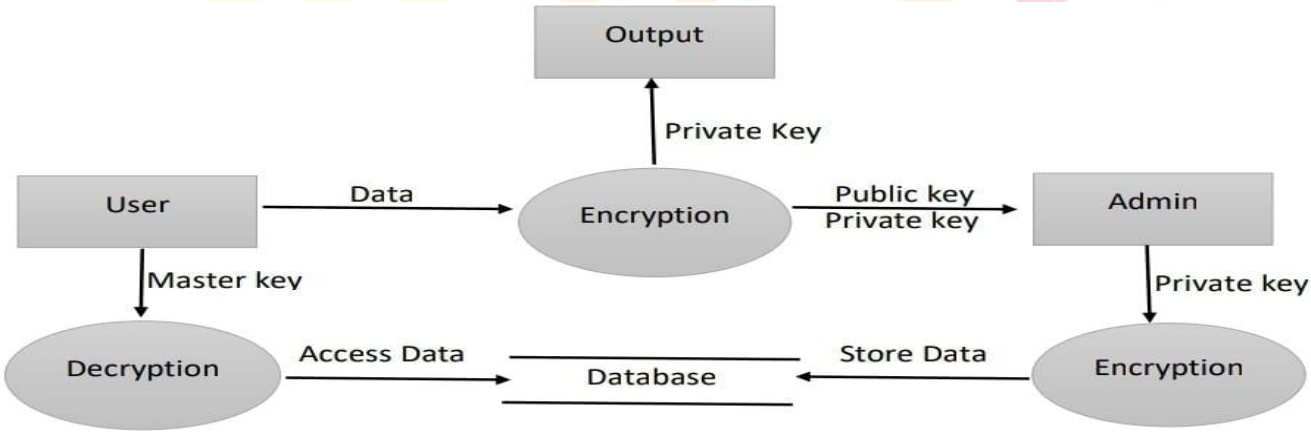

Fig. 1

NETWORK SECURITY

This project stands as a beacon of innovation in the realm of network security, heralding a transformative shift in password management practices. By seamlessly integrating cryptographic principles and OTP authentication, it not only bolsters security but also liberates users from the shackles of password memorization. This revolutionary solution dramatically mitigates the perennial risks associated with password-based vulnerabilities, fortifying network defenses with unwavering resolve.

AUTHENTICATION MECHANISM

The project relies on a one-time password (OTP) system, eliminating the need for users to memorize passwords. Upon accessing the application, users are prompted to enter a dynamically generated OTP, which serves as the primary means of authentication, ensuring both security and user convenience.

SYSTEM ARCHITECTURE

The developed application described in this paper is a password generator and locker system using cryptography.

1. **Login page**:
   Users have the option to log into the application via two distinct methods: either by utilizing a One-Time Password (OTP) system or by employing Google authentication. These authentication pathways offer users flexibility and security in accessing their accounts within the application.

2. **Password generator**
   i. Password hint
   ii. Random text

   Users are prompted to input a password hint along with random text to initiate the password generation process. Upon completion of these inputs, users can generate their password by selecting the 'Generate Password' option. This approach ensures an additional layer of security and aids users in creating robust passwords for their accounts

3. **Add password**
   i. User name
   ii. User email
   iii. Password

   The application provides users with the convenience of storing their generated passwords. Users also have the facility of modifying and deleting passwords.

CONCLUSION

This project presents a pioneering solution in password management, blending symmetric cryptography and OTP authentication to enhance security and user experience. By addressing the vulnerabilities inherent in traditional password-based systems, it sets a new standard for network security, poised to shape future authentication practices.

FUTURE SCOPE

- Advanced Password Management Features: Introducing features such as password strength assessment, password expiration reminders, and secure password sharing functionalities to provide users with comprehensive password management capabilities.
- Integration with Emerging Technologies: Exploring integration with emerging technologies such as blockchain for decentralized authentication mechanisms or artificial intelligence for adaptive security measures.
- User Feedback and Iterative Development: Soliciting and incorporating user feedback to continually refine and improve the application's usability, security, and feature set through iterative development cycles.
- Autofill password: No need to copy the password separately for each application or website.

REFERENCES

- https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers
- https://crypto.stanford.edu/~dabo/courses/cs255_winter24/hw_and_proj/proj1.pdf
- https://www.cnsnevada.com/what-is-the-memory-capacity-of-a-human-brain/#:~:text=As%20a%20number%2C%20a%20%E2%80%9Cpetabyte,2.5%20million%20gigabytes%20digital%20memory
- https://en.wikipedia.org/wiki/Symmetric-key_algorithm
- https://firebase.google.com/docs
- https://en.wikipedia.org/wiki/Challenge%E2%80%93response_authentication