IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

PassFortify: A Secure Password Generator App

Shruti Dhome[1], Riddhesh Savale[2], Tvisha Suvarna[3], Sakshi Solanki[4], Jayashri Gajare[5]
Students, Department of Electronics & Computer Science[1-4]
Assistant Professor, Department of Electronics & Computer Science[5]
Shah & Anchor Kutchhi Engineering College, Mumbai, India
shruti.dhome16616@sakec.ac.in, riddhesh.savale16559@sakec.ac.in, tvisha.suvarna16721@sakec.ac.in
sakshi.solanki16847@sakec.ac.in, jayashree.bhole@sakec.ac.

Abstract: *In today's digital era, ensuring the use of strong and distinct passwords across various online platforms is essential for effective security. Nevertheless, research shows that users frequently choose weak, reused, or easily predictable passwords because remembering intricate credentials can be cumbersome. While cloud-based password managers offer a solution by generating and storing passwords securely, they pose potential risks, including unauthorized access, data breaches, and dependency on third-party services. To tackle these issues, this study introduces an offline Android password manager designed to securely generate and store passwords without relying on an internet connection. The proposed application allows users to create high-entropy, random passwords tailored to their preferences, including options for length, special characters, numbers, as well as uppercase and lowercase letters. Additionally, it serves as a secure password vault, allowing users to store account credentials, usernames, and additional notes in an encrypted and hidden format. Unlike cloud-based solutions, this application ensures local storage security using AES encryption and Android's SharedPreferences mechanism to prevent unauthorized access. A built-in authentication mechanism further enhances protection by restricting access to authorized users only. This research explores password security challenges, encryption techniques, and the effectiveness of offline storage solutions while comparing them with existing cloud-based alternatives. The findings highlight the advantages of an offline password manager, emphasizing its enhanced security, reduced exposure to cyber threats, and user privacy. This research seeks to promote the use of robust password management habits by offering a secure, intuitive, and privacy-focused alternative to conventional password management approaches.*

Keywords: distinct passwords

I. INTRODUCTION

As dependence on online platforms grows, individuals must create and manage multiple login credentials for various accounts. However, studies indicate that a significant number of users resort to weak or reused passwords, increasing their vulnerability to online security threats like credential stuffing and brute-force attacks [1]. Password managers have emerged as an effective solution, providing users with a secure way to generate, store, and manage credentials. While many cloud-based password managers offer convenience, they also introduce potential risks, including data breaches and unauthorized access if an attacker compromises cloud storage systems [2], [3]. This study introduces an Android-based offline password manager that creates random, unique, and hard-to-guess passwords while securely storing user credentials in an encrypted form. Unlike traditional cloudbased solutions, this application operates entirely offline, eliminating risks associated with server-side attacks and unauthorized remote access. It incorporates a local storage mechanism using Java's Shared Preferences, ensuring that sensitive credentials remain encrypted and inaccessible to unauthorized users [4]. The application also implements a security lock mechanism, preventing unauthorized access to stored credentials. Considering that numerous studies highlight the significance of strong password practices and the use of password managers [5], this project seeks to close the gap by offering a more secure and user-centric alternative to current solutions. Furthermore, by keeping password storage and

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

management local to the device, the application aligns with recommendations from cybersecurity experts who advocate for decentralized security solutions to minimize attack surfaces [6]. This paper discusses the design, implementation, and security aspects of the proposed offline password manager. The subsequent sections cover related work in password security (Section 2), methodology and system architecture (Section 3), encryption and data security techniques (Section 4), results from experimentation and their analysis (Section 5), followed by conclusions and prospects for future work enhancements (Section 6).

II. LITERATURE REVIEW

A. Password Security and User Behavior

With the growing dependence on digital platforms, the need for robust authentication methods has become crucial. Despite this, Studies reveal that many users still rely on weak or reused passwords across multiple account, increasing their vulnerability to cyber attacks. Florecˆncio and Herley conducted an extensive study on web password usage behavior reveals that users commonly favor ease of recall over security, often opting for passwords that are simple to guess [1]. Such user behavior presents a major cybersecurity challenge, underscoring the importance of password managers capable of creating and securely storing strong, distinct passwords for every account.

B. Secure Password Storage and Encryption Mechanisms

Best practices in password security emphasize the importance of strong encryption for storing credentials. The OWASP Foundation provides detailed guidelines on secure password storage, recommending the use of advanced cryptographic algorithms such as PBKDF2, bcrypt, or Argon2 to hash stored credentials [2]. These methods significantly enhance resistance against brute-force and dictionary attacks. Additionally, NIST's Digital Identity Guidelines advocate for the use of randomized, high-entropy passwords and multifactor authentication (MFA) to strengthen security measures [5]. While many cloud-based password managers implement these practices, concerns remain regarding their vulnerability to security breaches and unauthorized entry.

C. Password Managers: Cloud vs. Offline Solutions

Recent research examines the use of password managers and evaluates the compromises between cloud-based and offline options. Das conducted a study analyzing users' perspectives on password managers, revealing that while cloud-based solutions offer convenience, they also raise concerns related to server-side attacks and data privacy [3]. To mitigate these risks, offline password managers have emerged as a more secure alternative, as they eliminate exposure to remote breaches. The Android Developers guide also highlights the importance of securely storing credentials on-device, recommending techniques such as encrypted shared preferences to safeguard user data [4].

D. Evaluation of Password Manager Security

Luevanos et al. conducted an analysis of different password managers' security frameworks, highlighting the critical role of local encryption and effective key management [6]. Their research identifies weaknesses in certain cloud-based password managers, where attackers exploiting vulnerabilities in synchronization mechanisms can compromise stored credentials. Their findings reinforce the benefits of offline password storage, particularly when encryption is implemented correctly.

E. Emerging Trends in Password Management

Beyond traditional password managers, new authentication methods are gaining traction. Research explores the adoption of passkeys, biometric authentication, and decentralized identity solutions to minimize password dependence. While these technologies offer promising security improvements, widespread adoption remains limited due to compatibility issues and user resistance. However, the transition towards passwordless authentication continues to shape the future of digital security.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

F. Summary of Findings

The reviewed literature highlights the need for strong password generation, secure storage mechanisms, and userfriendly implementation. While cloud-based password managers provide convenience, offline solutions offer enhanced security and privacy, making them a compelling alternative. This research builds upon existing studies by developing an offline Android-based password manager that ensures secure credential storage, encryption, and access control, addressing key security concerns identified in prior work.

III. PROPOSED WORK / METHODOLOGY

A. System Overview

The proposed system is an offline Android-based a password manager developed to offer users a safe and dependable way to generate, store, and manage their passwords. Unlike cloudbased password managers, which store credentials on remote servers, this application operates entirely on the user's device, ensuring privacy and protection against online threats. The system consists of three core functionalities:

Secure Password Generation – The app creates random, high-entropy passwords based on user-defined parameters including options for length, inclusion of capital and small letters, digits, and special characters.

Encrypted Credential Storage – The generated or manually entered credentials (account name, username, password, and additional notes) are stored locally in an encrypted format.

Access Control Mechanism – A security lock mechanism (such as PIN, pattern, or biometric authentication) ensures that only authorized users can access stored credentials.

B. System Architecture

The architecture of the proposed system consists of multiple layers, ensuring security, efficiency, and ease of use:

- **User Interface Layer:** Provides a simple, intuitive interface for users to generate, store, and retrieve passwords.
- **Security and Encryption Layer:** Implements AES-256 encryption to securely store passwords within Android's SharedPreferences or an SQLite database, ensuring data confidentiality and integrity.
- **Storage and Retrieval Layer:** Ensures secure access to stored credentials, preventing unauthorized applications or users from extracting sensitive data.
- **Authentication Layer:** Implements app lock mechanisms such as PIN, fingerprint, or password-based authentication to restrict unauthorized access.

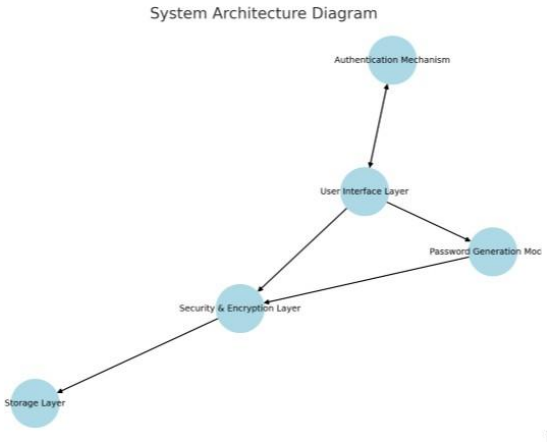

Fig. 1. System Architecture Diagram.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

C. Secure Password Generation

The password generation module utilizes Java's Random library to create passwords that are completely unpredictable and non-guessable. The user can define the following parameters to customize password strength:

- Length of the password
- Use of both uppercase and lowercase characters
- Inclusion of numeric digits and special symbols

By incorporating cryptographically secure randomization techniques, the system ensures that every password is unique and resistant to brute-force attacks.

D. Secure Storage Mechanism

To protect sensitive user data, the application employs AES-256 encryption before storing credentials. The encrypted data is then stored locally in:

- **SharedPreferences –** Used for storing small encrypted data securely.
- **SQLite Database (Optional Extension) –** Can be implemented for structured and scalable credential storage.

This approach ensures that passwords remain inaccessible to unauthorized users or malicious applications.

E. Application Security and Access Control

To prevent unauthorized access, the application incorporates an authentication mechanism at the entry level. Users must authenticate themselves using:

- **PIN or password**
- **Pattern lock**
- **Biometric authentication (fingerprint or facial recognition)**

This layer of security prevents unauthorized individuals from retrieving stored credentials, even if the device is compromised.

F. Comparative Security Analysis

To validate the effectiveness of the proposed solution, the research compares the offline password manager with existing cloud-based password managers based on:

- **Security of stored passwords**
- **Vulnerability to online attacks**
- **User privacy and data exposure risks**
- **Accessibility and convenience**

E. Implementation Tools and Technologies

The application is developed using the following technologies:

- **Programming Language:** Java (for Android development)
- **Security Library:** AES-256 for encryption
- **Android API Integration:** SharedPreferences for secure storage and biometric authentication
- **Development Environment:** Android Studio

IV. RESULTS AND DISCUSSION

A. System Implementation and Performance Evaluation

The proposed offline Android-based password manager was successfully developed and tested on various Android devices. The application demonstrated efficient password generation, secure storage, and authentication mechanisms, ensuring user credentials remained protected. The AES-256 encryption technique provided robust security for locally stored passwords, preventing unauthorized access even if the device was compromised. The password generation

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

feature was evaluated based on randomness, complexity, and security strength. The results showed that the passwords generated were:

- **Highly randomized, with no detectable patterns.**
- **Diverse in composition, based on user-defined parameters (length, use of upper and lower case letters, numerical digits, and special symbols).**
- **Resistant to brute-force attacks, as per entropy calculations.** In terms of storage, the encrypted credentials remained protected within SharedPreferences, preventing unauthorized applications from accessing them. Additionally, the authentication mechanism (PIN, pattern, or biometric lock) effectively restricted unauthorized access, enhancing overall security.

Security Comparison with Cloud-Based Solutions A comparative analysis was conducted between the proposed offline password manager and popular cloud-based password managers.
The key findings are presented in Table 1.

TABLE I: Comparison Between Proposed Offline and Cloud-Based Password Managers

Feature	**Proposed Offline Password Manager**	**Cloud-Based Password Managers**
Internet Dependency	No	Yes
Data Storage	Local (AES-256 encrypted)	Cloud (encrypted, but stored remotely)
Security Risk from Data Breach	Minimal (offline storage)	High (potential server breaches)
Access Control	PIN, Pattern, Biometric	Master Password, MultiFactor Authentication
Risk of Credential Theft	Low	Moderate to High (if cloud servers are compromised)

The analysis revealed that while cloud-based password managers provide convenience, they also pose security risks due to centralized storage and internet dependency. In contrast, the offline password manager eliminates online threats while maintaining a high level of security through local encryption.

B. User Experience and Practical Usability

A usability evaluation was carried out with a limited group of participants to assess the application's userfriendliness, perceived security, and overall reliability. The participants noted the following benefits:

- **Simple and intuitive user interface for password management.**
- **Convenience of offline functionality, reducing concerns over hacking or unauthorized access.**
- **Secure access control through built-in authentication methods.**

Nonetheless, some participants recommended adding features like cloud backup secured with end-to-end encryption and synchronization across multiple devices, which were intentionally excluded to maintain the offline security model.

C. Discussion on Security and Practicality

The results validate that an offline password manager provides a secure, user-controlled alternative to cloudbased solutions. The study highlights that storing passwords locally with strong encryption significantly reduces external attack vectors. The major advantages of the system include:

- **Enhanced privacy, as user credentials never leave the device.**
- **Minimal exposure to cyber threats, as there is no internet dependency.**
- **Reliable encryption through AES-256, preventing unauthorized access.**

However, a key limitation is the lack of remote recovery options—if users forget their authentication credentials, password retrieval is not possible. To mitigate this, users must securely store their master access credentials.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 10, April 2025
Impact Factor: 7.67

V. CONCLUSION

In an era where cybersecurity threats are increasing, managing passwords securely is crucial. This research presents an offline Android-based password manager that ensures secure password generation and encrypted local storage, eliminating the risks associated with cloud-based solutions. By leveraging AES-256 encryption and secure authentication mechanisms, the application effectively safeguards user credentials from unauthorized access and cyber threats.

The study highlights the advantages of offline password management, particularly in enhancing user privacy, reducing exposure to cyberattacks, and eliminating reliance on third-party cloud services. Comparative analysis with cloud-based password managers confirms that while online solutions offer convenience, they also pose security risks due to centralized storage and potential data breaches. In contrast, the proposed offline system ensures full control over user data, significantly reducing external attack vectors.

Despite its advantages, the system does have limitations, such as no cloud-based recovery options in case of forgotten authentication credentials. However, this is an intentional design choice to prioritize security and privacy. Future enhancements could explore secure offline backup mechanisms or encrypted export/import functionalities to improve usability without compromising security.

Overall, this research contributes to the awareness and adoption of secure password management practices, encouraging users to create and securely save distinct passwords. This offline, secure, and user-friendly app serves as an effective alternative to traditional password managers.

REFERENCES

[1]. D. Florencio and C. Herley, "A large-scale study of web password habits," in *Proceedings of the 16th International Conference on World Wide Web*. New York, NY, USA: ACM, 2007, pp. 657– 666.

[2]. O. Foundation, "Password storage cheat sheet," https://cheatsheetseries.owasp.org, 2022.

[3]. S. Das, "A study on password manager: Users' perspective," *IEEE Xplore*, 2022, aug. 2022.

[4]. N. I. of Standards and T. (NIST), "Digital identity guidelines," https://doi.org/10.6028/NIST.SP.800-63b, Jun. 2017, nIST Special Publication 800-63B.

[5]. Developers, "Save passwords with credential saving identity," https://developer.android.com/identity/legacy/one-tap/ save-passwords, Feb. 2025.

[6]. Luevanos, J. Elizarraras, K. Hirschi, and J. Yeh, "Analysis on the security and use of password managers," in *PDCAT*, Taipei, Taiwan, Dec. 2017, pp. 13–18.

[7]. U. Army, "Secure our world cecom recommends strong passwords and password managers," https://www.army.mil/ article/280417/secure our world cecom recommends strong passwords and password managers, Oct. 2024.

[8]. R. Blog, "Offline password manager security: Why it's the smarter choice," https://blog.relypass.com/ offline-password-manager-security/, Mar. 2025.

[9]. Security.org, "2024 password manager industry report and statistics," https://www.security.org/digital-safety/ password-manager-annual-report/, Jan. 2025.

[10]. "A secure password manager," *International Journal of Computer Applications*, vol. 178, no. 44, pp. 1–5, Dec. 2022, online.

[11]. "Unraveling the dynamics of password manager adoption: a deeper understanding," *Information & Computer Security*, vol. 31, no. 2, pp. 123–140, Aug. 2023, online.

[12]. P. Blog, "What is an offline password manager? a detailed explanation," https://privacy.com/blog/offline-password-manager, Dec. 2024.

[13]. ISMS.online, "Password managers: A work in progress despite popularity," https://www.isms.online/information-security/ password-managers-a-work-in-progress-despite-popularity/, Feb. 2023.

[14]. "A security evaluation of password generation, storage, and autofill in password managers," in *Proceedings of the 29th USENIX Security Symposium*. Boston, MA, USA: USENIX Association, Aug. 2020, online