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

DOI: 10.48175/IJARSCT-25680