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 6, Issue 4, March 2026
Impact Factor: 8.2

KeyGo – A Secure Open-Source Password Manager for Android

Shree Pramod Indulkar[1], Prasad Ankush Kokate[2], Chetana Sanjay Chaudhary[3]
Students, Department of Computer Engineering[1-2]
Guide, Department of Computer Engineering[3]
Rasiklal M. Dhariwal Institute of Technology, Pune, India

Abstract: *In the modern digital age, users have numerous accounts on a plethora of online services that require managing many passwords and private data. The use of weak and repetitive passwords by many users or the storage of credentials in an insecure password location raises security concerns leading to account takeover, data breaches, and cyber-attacks. In this work, we introduce KeyGo, an Android-based secure but lightweight password manager application. Yeah, the app allows users to store passwords and credit card info locally on their devices without using cloud services and secures it all with encryption. For stored data, KeyGo implements AES-256 encryption, while password verification is performed using SHA-256 hashing. The application uses Kotlin and Android Architecture components with Material Design 3, Room Database to build a modern, responsive, friendly-user interface. Users can also unlock the vault via fingerprint or facial recognition, thanks to biometric authentication built into the system. The app is built on an offline-first architecture, which means that everything gets persisted on the user's device. This reduces risks related to cloud storage and improves privacy. The findings show that the system achieves secure storage, simple management of passwords and file encryption as part of a user- friendly GUI*

Keywords: *online services*.

DOI: 10.48175/568