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*.

I. INTRODUCTION

As online services developed rapidly, users had to maintain several accounts in banking institutions, social media outlets, e-payment sites and enterprise applications. All of these accounts require proper authentication credentials, mostly in the form of passwords. Unfortunately, for most users, remembering several complex passwords is going to be a challenge and will most probably end up in weak passwords or reused passwords. This poses a heavy exposure to cyber-attacks, identity theft scams and unauthorized access to data.

One way to securely store and manage user credentials is through the use of password managers. These systems save and encrypt sensitive information, then users can use a master password to retrieve the data. Yet most current password management solutions are cloud-based, which some might have concerns regarding the privacy of their data or potential hacks on a server level.

Love your passwords, but hate not remembering them all? The KeyGo Password Manager is here to help: a fully offline and privacy-savvy password manager for Android devices. It securely stores passwords, bank card numbers, and files with content encrypted with strong algorithms. There is full control of sensitive information by users, as all data does not leave the user's smartphone.

Mobile application is written in Kotlin and Android Jetpack components with the MVVM architecture pattern for better maintainability, scalability. Security: It uses AES-256 encryption and SHA-256 hashing, along with biometric authentication.

The primary goal of this project is to develop a password management system that allows users to store their sensitive information securely while minimizing the dependence on any cloud infrastructure, providing secure and easy-to-use tool for managing confidential data.

DOI: 10.48175/568

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

II. LITERATURE REVIEW

A few password management solutions have since then been created to assist users in safely storing and securely handling credentials. These include traditional password managers like browser-based systems that allow users to store partial login details directly in the browser environment. These are convenient solutions, but they often fall short in terms of strong encryption mechanisms and can expose user data if the device is compromised.

Please note that while building password managers like Bitwarden, LastPass and KeePass newer security mechanisms such as encryption and synchronization over different devices are roborated. These systems keep user passwords securely encrypted, and use the master password that users set to access them. Many of these solutions rely on cloud servers to synchronize, which gives rise to potential privacy issues.

In the mainstream, mobile password managers tailored for Android platforms have also achieved significant popularity. Local storage and encryption algorithms protect user credentials from these applications. What's the catch, you ask: Most of the existing apps are either too advanced or tend to require stable internet access.

It highlights, on Studies Some research focuses more on the aspect of user-friendly interfaces in password management systems, local encryption (information or data is encrypted locally before it's sent through a network) and strong authentication mechanisms. One of the common encryption algorithm is AES(Advanced Encryption Standard) with good security and efficiency it is commonly used to encrypt sensitive information.

Drawing on the findings of these studies, the KeyGo system aims to offer a lightweight, offline-first password manager that combines robust encryption, biometric authentication and an intuitive user experience for better usability and security.

III. RESEARCH GAP

Many password managers are available, however they have their limitations. Numerous applications run on the basis of cloud storage which led to risks like server breach, unauthorized access and privacy issue. Consumers concerned with data privacy may prefer solutions that allow sensitive user information to remain stored only on personal devices.

A major weakness of existing password managers is the absence of integrated file encryption capabilities. Most password managers do a single job: they store your login credentials, but people usually need to keep other sensitive data like documents or images safe.

Moreover, some password managers have very complicated user interfaces which are fresh of use for novice users. Hence, we need a simple and lightweight password manager which is also privacy-focused.

The KeyGo system aims to address these gaps by providing:

- Fully offline password management
- AES-256 encryption for strong data protection
- Biometric authentication for convenient and secure access
- Encrypted file storage for protecting sensitive files
- **A** simple and intuitive user interface

IV. METHODOLOGY

KeyGo Application development follows a methodical approach of requirement analysis, system design, implementation and testing.

Requirement Analysis

During this phase, the requirements of the system which are both functional and non-functional are identified. Must allow users to have a secure storage method for passwords, credit card information and encrypted files. It must offer robust security mechanisms: encryption, authentication and automatic locking.

System Design

The application is structured following the MVVM architecture, which divides up an app into three layers:

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

1) Model Layer – Handles data storage and database operations using Room Database.
2) View Layer – Displays the user interface using Material Design components.
3) ViewModel Layer – Manages application logic and communication between the UI and database.

Implementation

It is an Android application written in Kotlin. The UI is built with XML layouts and Material Design 3 UI components. For local storage of encrypted data, the system makes use of the Room Database. In addition, things such as passwords and credit card numbers are stored using AES-256 encryption in the database. This means that the master password is hashed using SHA-256.

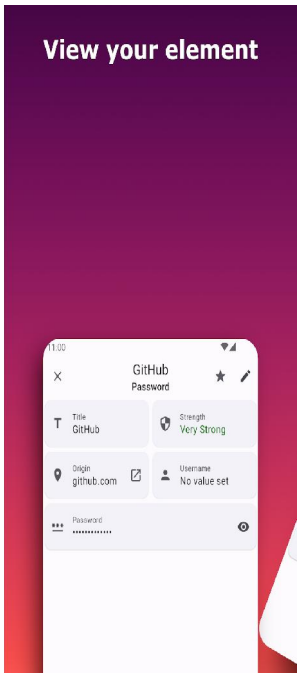
Testing

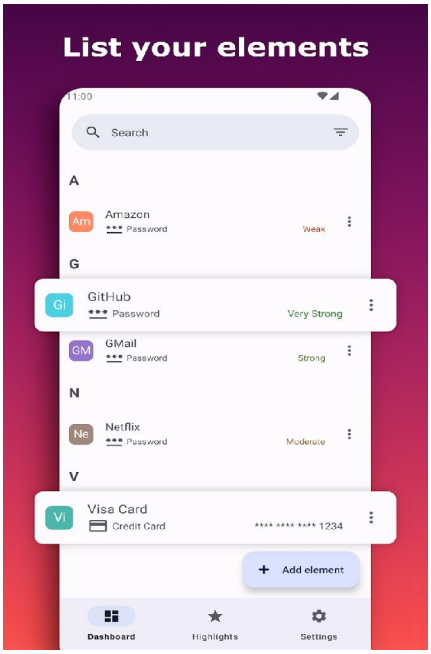
We test the system with various testing methods, such as:

• Unit Testing using JUnit
• AndroidX Test for Instrumentation Testing
• UI Testing using Espresso

Testing ensures all the features work as they should, and sensitive data remains encrypted and secure.

V. RESULTS AND DISCUSSION:





The KeyGo password manager application was successfully developed and tested on Android devices. The application provides a secure and user-friendly platform for managing sensitive information. Users can store passwords, credit card details, and encrypted files within a secure vault protected by a master password and biometric authentication. The AES-256 encryption mechanism ensures that all stored data remains protected even if the device is accessed by unauthorized users. The user interface developed using Material Design 3 provides a modern and intuitive experience. Users can easily add, edit, search, and delete stored credentials. The application also supports dark mode for improved usability. The offline-first architecture ensures that the system works without internet connectivity, providing enhanced privacy and reliability. The experimental results show that the system successfully meets its design goals by providing strong security, efficient performance, and an easy-to-use interface.

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

VI. CONCLUSION

This research presented **KeyGo**, a secure and lightweight password manager designed for Android devices. The system provides a reliable solution for managing sensitive information such as passwords, credit card details, and encrypted files. By using **AES-256 encryption**, **SHA-256 hashing**, and **biometric authentication**, the system ensures a high level of security and privacy. The offline-first architecture eliminates the risks associated with cloud storage and gives users full control over their data. The application demonstrates how modern Android technologies such as **Kotlin, Room Database, and MVVM architecture** can be used to develop secure and scalable mobile applications. Future improvements may include password breach detection, secure backup options, and cross-device synchronization while maintaining strong privacy protections.

VII. ACKNOWLEDGMENT

The successful completion of this research work would not have been possible without the guidance and support of our project guide and faculty members of the Department of Computer Engineering. Their valuable suggestions, encouragement, and technical knowledge greatly contributed to the development of this project. We would also like to express our sincere gratitude to our institution for providing the necessary resources, infrastructure, and academic support required to complete this research successfully.

REFERENCES

[1]. Kotlin Programming Language – JetBrains Documentation
[2]. NIST. Advanced Encryption Standard (AES) Specification
[3]. Android Jetpack Architecture Components Documentation
[4]. SQLite and Room Database Documentation
[5]. OWASP Mobile Security Guidelines
[6]. Google Material Design Guidelines
[7]. Android Developers Documentation – https://developer.android.com