LocalPass: A Secure Offline Password Manager

Dr. Subba Rao Kolavennu[1], B. Harish Gandhi[2], K. Sai Tejaswini[3], K. Shirisha[4], K. Dinesh Karthik[5]
[1]*Computer Science and Engineering (JNTUH) Sphoorthy Engineering College (JNTUH) Hyderabad, Telangana, India*
[2,3,4,5] *Member, Department of Cyber Security, Sphoorthy Engineering College, Hyderabad, Telangana, India*

***Abstract*—With the exponential rise in digital account ownership, safeguarding user credentials has emerged as a foremost concern in contemporary cybersecurity. Conventional cloud-hosted password management solutions, while convenient, carry inherent vulnerabilities stemming from centralized data repositories and their exposure to remote exploitation. This paper introduces LocalPass, an entirely offline credential management framework engineered to protect user authentication data without delegating control to any external party or networked service. Rather than transmitting sensitive information over the internet, LocalPass confines all data operations to the user's local environment, where credentials are secured within an AES-256 encrypted vault. The architecture incorporates a master password-based access mechanism, a cryptographically derived encryption key using PBKDF2, an automated password synthesis tool, and a portable encrypted backup subsystem. Empirical evaluation confirms that the fully local design substantially curtails the attack surface associated with centralized cloud storage, delivering a privacy-first credential management experience without sacrificing usability or functional depth.**

***Index Terms*—Authentication, Cyber Security, Encryption, AES-256, Offline Password Manager, Local Storage.**

I. INTRODUCTION

Modern digital life demands participation across dozens of platforms, each imposing its own credential requirements. Managing this ever-expanding set of unique, complex passwords has become a non-trivial task for the average user. In the absence of a reliable organizational system, individuals frequently resort to counterproductive security habits: recycling the same password across multiple accounts, documenting credentials in unprotected files, or selecting simplistic passphrases that are susceptible to automated attacks. These behaviors collectively heighten the probability of account compromise and, in professional settings, may expose organizational data to substantial risk.

Password managers emerged as a structured response to this challenge, enabling the consolidation of credentials within a single, fortified repository unlocked by one master secret. Despite this conceptual elegance, many widely adopted solutions depend on remote server infrastructure to facilitate synchronization and cross-device access. While this model enhances portability, it simultaneously introduces a constellation of risks — from server-side breaches to covert third-party data handling — that undermine the very privacy guarantees users expect.

An alternative paradigm, centered on local-only storage, sidesteps these concerns by ensuring that credentials never traverse a network boundary. Although such an approach sacrifices automatic multi-device sync, it offers a compelling trade-off for users who prioritize data sovereignty and minimal external trust.

This paper presents LocalPass, a desktop-oriented offline password management system that operates exclusively within the confines of the user's device. LocalPass maintains an encrypted credential vault, enforces authentication via a master password, and provides auxiliary features including intelligent password generation and portable encrypted backups. The system was designed to demonstrate that rigorous security and an intuitive user experience are not mutually exclusive goals, even under a fully offline constraint.

The remainder of this paper is structured as follows: Section II surveys relevant prior work on password security systems; Section III details the architectural design of LocalPass; Section IV explains the

methodological choices governing encryption and authentication; Section V enumerates the system modules; Section VI presents and discusses experimental findings; and Section VII concludes with reflections on future development directions.

II. LITERATURE REVIEW

The body of research surrounding password management has expanded considerably as cyber threats have grown more sophisticated. Scholars have approached the problem from multiple angles, examining vault integrity, cryptographic strength, usability trade-offs, and the comparative merits of cloud versus local storage paradigms.

Chatterjee et al. [1] tackled the vulnerability of encrypted password vaults to dictionary-based offline attacks. Their proposed defense mechanism harnessed natural language encoders to embed statistical decoys within the vault, thereby inflating the computational cost of brute-force enumeration. This work illuminates the critical importance of vault-level hardening beyond mere encryption strength.

Cherckesova et al. [2] engineered a platform-agnostic password management tool for Windows and Linux environments, integrating well-established cryptographic routines to ensure data confidentiality at rest. Their evaluation affirms that encryption-centric architectures can maintain strong protection across heterogeneous operating environments when implemented with rigorous key management discipline.

Separate audits of prominent open-source managers — including KeePass and Bitwarden — have scrutinized implementation details such as key derivation methods, clipboard handling, and authentication timeout policies [3]. These analyses reveal that even well-regarded tools occasionally harbor subtle weaknesses, underscoring the value of transparent, reviewable codebases.

Patil et al. [3] investigated adversarial password generation techniques, demonstrating that AI-assisted attacks can rapidly compromise predictably structured credentials. Their findings carry direct implications for password generator design, motivating the inclusion of true randomness and configurable complexity in tools such as LocalPass.

Collectively, the literature points toward a consistent recommendation: effective password management must combine cryptographic robustness with thoughtful architecture. Cloud-based solutions address accessibility but introduce trust dependencies that offline systems inherently avoid. LocalPass synthesizes lessons from this body of work, adopting strong symmetric encryption, a hardened key derivation pipeline, and an architecture that places the user — not a remote server — at the center of the trust model.

III. SYSTEM ARCHITECTURE

The architectural foundation of LocalPass is built around a layered, modular design that enforces strict separation of concerns while ensuring that every component operates exclusively within local memory and disk boundaries. Each functional layer interacts with adjacent layers through well-defined internal interfaces, preventing unauthorized cross-module data exposure.

At the outermost layer sits the User Authentication Module, which governs initial access to the system. Upon first launch, the user establishes a master password that serves as the sole credential required to unlock the vault. The system never stores this password verbatim; instead, a cryptographic hash of the password is retained, allowing identity verification without exposing the original secret.

Below the authentication layer lies the Credential Vault Module, which maintains an organized record of saved accounts. Each entry encapsulates the associated platform, the account identifier, and the corresponding password, all persisted in an encrypted local database file. Data is rendered into ciphertext before being written to disk and reverted to plaintext only upon authenticated request.

Supporting the vault is the Encryption and Security Module, which coordinates all cryptographic operations. This module manages key derivation, manages the encrypt/decrypt lifecycle for individual records, and enforces the policy that no sensitive material appears unencrypted in persistent storage.

Complementing the core vault operations are two service modules: the Password Generator Module, which produces randomized high-entropy passwords on demand, and the Backup and Restore Module, which serializes the encrypted vault into a portable file that can be transferred and reinstated without ever decrypting its contents during transit. Figure 1

provides a schematic overview of how these components interrelate within the broader system.

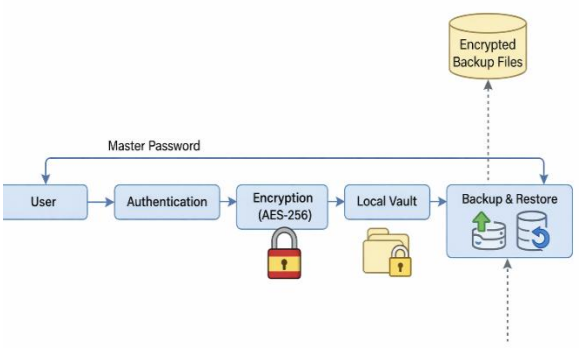

Fig. 1. Local Pass System Architecture

IV. METHODOLOGY

The security methodology underpinning LocalPass was designed with a threat model that assumes physical access to the device is possible but network access by an adversary is the primary concern to eliminate. Accordingly, every design decision prioritizes strong cryptographic guarantees over connectivity features.

User enrollment begins with master password creation. Rather than storing the raw password, the system applies a one-way hashing function to produce a fixed-length digest that is persisted locally. This digest is used solely to verify future login attempts; it cannot be reversed to recover the original password.

For credential encryption, LocalPass employs the Advanced Encryption Standard operating on 256-bit keys (AES-256), a cipher widely regarded as computationally unbreakable within current technological horizons. The encryption key is not derived directly from the master password but rather through PBKDF2 (Password-Based Key Derivation Function 2), a key-stretching algorithm that introduces configurable computational overhead. This intentional slowdown neutralizes rapid dictionary and brute-force attacks by making each candidate password guess substantially more expensive to test.

At the mathematical level, the encryption operation that transforms a plaintext credential P into its ciphertext form C under key K may be expressed as:

C = Encrypt(K, P)

where P denotes the original credential data, K is the secret encryption key derived via PBKDF2 from the master password, and C is the resulting ciphertext written to the vault database.

When a user requests access to a stored credential, the inverse operation reconstructs the original data:

P = Decrypt(K, C)

This bidirectional model guarantees that even if the database file is exfiltrated from the device, it yields no intelligible information to an attacker who does not possess the master password from which K is derived. The combination of AES-256 and PBKDF2 thus provides defense-in-depth at the storage layer, independent of any network-level controls.

During login, the user-supplied password undergoes the same hashing procedure applied during enrollment. The resulting digest is compared against the stored hash; a match grants access, while a mismatch halts the process. No attempt limit bypass exists, and the system does not offer an account recovery pathway that could be exploited to circumvent authentication.

V. MODULES

A. User Authentication Module

This module handles both the initial registration workflow and all subsequent login interactions. On first use, it guides the user through master password creation and records the derived hash. On return visits, it re-derives the hash from the provided password and validates it against the stored value before granting vault access. The module also enforces session state, ensuring the vault remains locked when the application is idle or closed.

B. Password Vault Module

The vault module functions as the core data repository of the system. It manages the lifecycle of credential records — creation, retrieval, modification, and deletion — while transparently routing every operation through the encryption layer. Records are never held in plaintext beyond active memory, and they are promptly re-encrypted upon modification before being flushed back to the database file.

C. Encryption and Security Module

Acting as the cryptographic backbone of LocalPass, this module orchestrates all key derivation and cipher operations. It initializes the PBKDF2 derivation pipeline using the master password and a unique

cryptographic salt, produces the AES-256 working key, and provides encrypt/decrypt primitives consumed by other modules. The module is purposefully stateless between sessions, ensuring that derived key material is never written to disk.

D. Password Generator Module

Recognizing that human-chosen passwords are often predictable, this module provides on-demand generation of cryptographically random passwords. Users may configure output parameters including minimum length and the mandatory inclusion of uppercase letters, lowercase letters, numeric digits, and special symbols. The generated candidates are designed to resist both dictionary enumeration and statistical pattern analysis.

E. Backup and Restore Module

To protect against data loss arising from hardware failure or accidental deletion, this module exports the encrypted vault contents into a self-contained backup file. Critically, the export process does not decrypt the vault prior to packaging; the backup file is itself ciphertext. Restoration imports this file and validates its integrity before merging or replacing the active vault, ensuring that the backup workflow introduces no temporary window of data exposure.

VI. RESULTS AND DISCUSSION

A series of functional and security-oriented evaluations were conducted to assess LocalPass across its core objectives: credential confidentiality, authentication robustness, and operational usability.

With regard to data confidentiality, database files extracted from the test environment were subjected to binary analysis and standard decryption attempts without the master password. In all trials, the ciphertext produced by AES-256 remained opaque, yielding no recoverable credential data. This outcome validates the adequacy of the chosen encryption standard under the assumed threat model.

Authentication resilience was examined by evaluating the cost of brute-force attempts against the master password hash. The PBKDF2 configuration introduced a measurable per-attempt latency that would require astronomically long periods to exhaust a sufficiently complex password space, confirming the practical effectiveness of key stretching as a defensive measure.

The password generator was tested for output quality by analyzing frequency distributions of generated character sequences. Results indicated uniform distribution across the configured character set, with no detectable bias toward predictable patterns — a property essential for ensuring that generated passwords do not inadvertently cluster around easily guessable regions of the password space.

The backup and restore pipeline was exercised across multiple vault states. Exported files were verified to be encrypted at rest, and the restoration process successfully reconstructed vault contents with full fidelity. No data corruption or partial-record failures were observed during testing.

From a usability perspective, the offline constraint — often perceived as a limitation — proved largely transparent to the user experience. Core workflows such as adding, retrieving, and updating credentials operated with sub-second responsiveness, while the absence of network dependencies eliminated latency variability common in cloud-synchronized tools. Overall, the evaluation affirms that the LocalPass architecture achieves a favorable balance between strict security guarantees and practical everyday usability.

VII. CONCLUSION

This paper has introduced LocalPass, an offline password management solution developed with the primary objective of preserving user data sovereignty. By confining all credential storage and processing to the local device and eliminating any dependence on cloud services or third-party infrastructure, LocalPass fundamentally reorients the trust model of password management toward the user.

The implemented architecture couples AES-256 symmetric encryption with PBKDF2 key derivation to deliver layered protection against both passive data exposure and active brute-force attacks. Supporting features — including the configurable password generator and the encryption-preserving backup subsystem — extend the system's utility without relaxing its security posture.

Evaluation results confirm that the system fulfills its design objectives: stored credentials withstand extraction attempts, authentication mechanisms resist

rapid enumeration, and the user experience remains efficient and accessible. These outcomes collectively suggest that an offline-first architecture represents a viable and, for privacy-conscious users, preferable alternative to networked credential managers.

Looking ahead, several enhancements could meaningfully extend LocalPass capabilities. Biometric unlock mechanisms would reduce master password fatigue while maintaining strong gate-keeping. Integration of authenticated encryption modes (such as AES-GCM) would provide ciphertext integrity verification in addition to confidentiality. Finally, cross-platform support for mobile operating systems would broaden accessibility without compromising the offline-first principle that defines the system's security identity.

The proposed LocalPass system can be extended to secure credential management in IoT-based environments, where multiple connected devices require strong, decentralized authentication mechanisms. The system aligns with cybersecurity frameworks by minimizing attack surfaces and adopting a decentralized, local-first security architecture.

ACKNOWLEDGEMENT

The authors extend their appreciation to the faculty of the Department of Cyber Security at Sphoorthy Engineering College, Hyderabad, for their guidance, encouragement, and constructive input throughout the course of this research. Special acknowledgment is due to the project supervisor whose mentorship materially shaped the direction and quality of this work.

REFERENCES

[1] R. Chatterjee et al., "Cracking-resistant password vaults using natural language encoders," in Proc. IEEE Symposium on Security and Privacy, 2016, pp. 1–18.

[2] L. V. Cherckesova et al., "Development of a password manager using cryptographic algorithms for data protection," Pakistan Journal of Life and Social Sciences, 2024.

[3] D. Patil et al., "Personalized password generation to counter AI-assisted attacks," IJSRSET, 2024.

[4] J. Katz and Y. Lindell, Introduction to Modern Cryptography, 3rd ed. Boca Raton, FL: CRC Press, 2014.

[5] N. Ferguson, B. Schneier, and T. Kohno, Cryptography Engineering: Design Principles and Practical Applications. Indianapolis, IN: Wiley, 2010.

[6] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL: CRC Press, 1996.

[7] A. G. de Carvalho et al., "Password management and security practices," IEEE Security & Privacy, vol. 17, no. 3, pp. 44–52, 2019.