IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cred-Safe

[1]Saila S, [2]Anuroopa Shankar, [3]Saniya Taj A [4]Dhanusha R,[5]Neha

[1]Asst. Professor, [2]Student, [3]Student,[4]Student, [5]Student

[1]Information Science & Engineering,

[1]T John Institute of Technology, Bangaluru, India

Abstract: CRED SAFE is a powerful and secure open-source password manager created to address the growing need for robust password security in an era of increasing cyber threats. Its primary goal is to simplify the process of generating, storing, and managing passwords, enabling users to protect their digital identities with ease. The customizable password generator is a standout feature, allowing users to create strong, random passwords tailored to specific requirements, such as length and the inclusion of character types like uppercase and lowercase letters, numbers, and special symbols. This ensures the creation of passwords that are resistant to brute force and dictionary attacks. CRED-SAFE also offers a highly secure storage solution, leveraging end-to-end AES encryption to protect saved credentials from unauthorized access. The intuitive interface makes it simple for users to view, edit, or delete stored passwords as needed, ensuring a seamless user experience. To further enhance security, the platform includes features such as two-factor authentication, adding an extra layer of protection against potential breaches.

By combining advanced password generation, encrypted storage, and user-friendly management tools, CRED SAFE empowers users to adopt better password practices, significantly reducing risks associated with weak or predictable passwords. Whether it's for personal use or managing multiple accounts across various platforms, CRED SAFE provides a reliable solution for maintaining strong and secure authentication credentials, ensuring safer online experiences for all users.

I. INTRODUCTION

CRED-SAFE is a secure software tool designed to address the growing need for strong password management in the face of increasing cyber threats. It simplifies the creation and management of robust passwords, ensuring high levels of digital security. By using a cryptographically secure random number generator (CSPRNG), CRED-SAFE generates highly unpredictable passwords with high entropy, making them resistant to brute-force attacks, dictionary attacks, and social engineering attempts.

The tool allows users to customize password characteristics, such as length, inclusion of uppercase and lowercase letters, numbers, and special characters, while avoiding common, easily guessed patterns like “123456” or “password.” This ensures that passwords meet modern security standards while being tailored to user preferences.

CRED-SAFE integrates seamlessly with password managers for secure storage and retrieval of credentials and supports multi-factor authentication (MFA) to add an extra layer of protection to user accounts. By automating the process of password creation and storage, CRED-SAFE promotes better security practices, reduces the risks of weak or reused passwords, and empowers users to safeguard their online accounts effectively.

RESEARCH METHODOLOGY

The research methodology outlines the systematic approach undertaken to design, develop, and evaluate the password manager. The methodology is divided into the following phases

Requirement Analysis

- Conduct a literature review to identify gaps in existing password management solutions and analyze current cybersecurity threats.
- Use surveys or interviews to gather user insights on challenges and expectations related to password creation and management.

Design and Development

- Develop a secure system architecture incorporating features like AES encryption for secure storage, cryptographically secure random number generation (CSPRNG) for password creation, and customizable options for password length and complexity.
- Integrate multi-factor authentication (MFA) and user-friendly interfaces to enhance security and usability.

Testing and Validation

- Perform functionality testing to ensure all features work as intended and security testing to identify and mitigate vulnerabilities using penetration tests.
- Conduct usability testing with target users to optimize the interface and improve the overall user experience.

Deployment and Evaluation

- Launch a beta version to a controlled group of users for feedback and optimization before the final release.
- Evaluate the tool's effectiveness in improving password security and user adoption through feedback and comparative analysis with existing solutions.

System Workflow

User Registration and Authentication

- User creates an account with a master password (hashed and securely stored).
- Logs in using the master password and optional multi-factor authentication (MFA).

Password Generation

- User defines parameters (length, character types) for a new password.
- System generates a strong, random password using secure algorithms.

Password Storage

- Generated or custom passwords are encrypted and saved securely with metadata (e.g., account name, URL).

Password Retrieval and Management

- Users can search, view, edit, or delete stored passwords.
- Decryption occurs only when a password is retrieved, ensuring security.

Security Enhancements

- Features like password strength checking, auto-lock, and data breach alerts ensure ongoing protection.

Key Features

CRED-SAFE incorporates the following core features to address the unique needs of users:

Strong Password Generator

- Creates secure, random passwords with customizable options for length and character types, ensuring robust security.

Secure Encryption

- Encrypts stored passwords and metadata with advanced encryption standards (e.g., AES), ensuring data protection.

Multi-Factor Authentication (MFA)

- Adds an extra layer of security to user accounts by requiring OTPs, biometrics, or hardware tokens during login.

Cross-Platform Synchronization

- Synchronizes encrypted passwords across devices for seamless access anytime, anywhere.

Password Autofill

- Automatically fills in login credentials for websites and apps, improving convenience and accuracy.

Data Breach Alerts

- Notifies users if their saved credentials are detected in known data breaches or leaks.

User-Friendly Interface

- Offers an intuitive and easy-to-use interface for storing, retrieving, and managing passwords effectively.

Backup and Recovery

- Provides options for encrypted backups and secure recovery mechanisms for lost credentials

Auto-Lock and Timeout

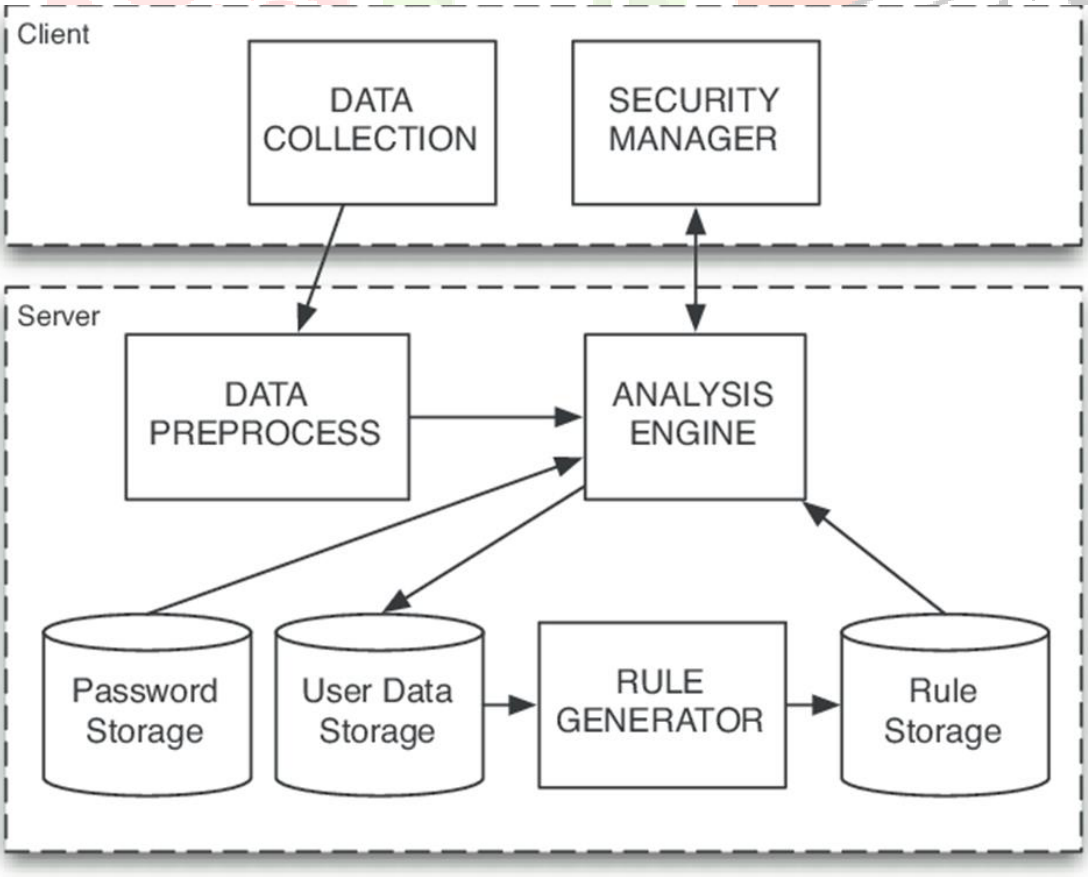
- Automatically locks the application after inactivity to prevent unauthorized access.

Integration

- Compatible with web browsers, mobile devices, and third-party tools for seamless use.

Architecture Analysis of CRED-SAFE

The architecture of a CRED-SAFE emphasizes security, usability, and scalability. By integrating encryption, authentication, and user-friendly interfaces, it ensures that users can securely generate, store, and manage their passwords while mitigating common cybersecurity threats.



Client-Side Components

- **User Interface (UI)**:
  - Provides a user-friendly interface for password creation, retrieval, and management.
  - Includes features like a dashboard, password strength meter, and autofill options.
- **Local Encryption and Decryption**:
  - Encrypts passwords locally on the user's device using algorithms like AES-256 before storage or transmission.
  - Ensures that passwords are decrypted only when needed and never sent in plaintext.
- **Password Generator**:
  - Implements a cryptographically secure random number generator (CSPRNG) to create strong, unpredictable passwords.
  - Allows customization of password parameters like length, character sets, and exclusions

Backend Components

- **Database (Secure Storage)**:
  - Stores encrypted passwords and associated metadata (e.g., account names, URLs) in a secure, structured format.
  - May use relational (SQL) or non-relational (NoSQL) databases with encryption at rest.
- **Authentication Module**:
  - Verifies user credentials using the master password (hashed with algorithms like Argon2 or bcrypt).
  - Supports multi-factor authentication (MFA) for added security.
- **API Layer**:
  - Provides communication between the client-side application and backend services.
  - Ensures all API requests and responses are encrypted using TLS for secure transmission.
- **Synchronization Service**:
  - Synchronizes encrypted password data across devices via secure cloud storage or peer-to-peer connections.
  - Ensures data integrity during transmission and prevents unauthorized access.

Security Features

- **Encryption Framework**:
  - End-to-end encryption ensures that only the user can decrypt their passwords.
  - Encryption keys are derived from the master password, ensuring even the service provider cannot access user data.
- **Data Breach Monitoring**:
  - Integrates with external APIs (e.g., Have I Been Pwned) to monitor if stored credentials are compromised.
- **Auto-Lock Mechanism**:
  - Automatically locks the password manager after a period of inactivity to prevent unauthorized access.

Integration Layers

- **Browser Extensions**:
  - Enable autofill functionality and password capture for websites, ensuring seamless integration with web browsers.
- **Mobile Apps**:
  - Provide on-the-go access to passwords with support for biometric authentication like fingerprint or facial recognition.
- **Third-Party Integration**:
  - Allows integration with other applications, such as Single Sign-On (SSO) tools or secure sharing platforms.

Deployment and Scalability

- **Deployment Model**:
  - Can be deployed as a local application (offline mode), a cloud-based service, or a hybrid model.

- **Scalability**:
  - Designed to handle increasing users and stored data efficiently by leveraging cloud services for storage and synchronization.

Risk Analysis and Mitigation

- **Threats**:
  - Risks include phishing attacks, brute-force attacks, database breaches, and insecure API communication.
- **Mitigation**:
  - Employ strong encryption, rate-limiting for authentication attempts, secure API gateways, and regular security audits.

IV. RESULTS AND DISCUSSION

1. Results

The development and testing of **CRED-SAFE** yielded significant results that validate its effectiveness and usability. Key outcomes are as follows:

1. **Enhanced Security**
   - Strong, unique passwords reduce vulnerability to attacks.
   - Encryption ensures secure storage of credentials.
2. **Improved Usability**
   - Simplifies managing multiple passwords with autofill and retrieval features.
   - Reduces the need to remember or reset passwords.
3. **Efficiency Gains**
   - Saves time in login and password recovery.
   - Synchronizes passwords across devices for seamless access.
4. **Risk Mitigation**
   - Alerts users of data breaches and ensures proactive password updates.
   - Minimizes risks of phishing and unauthorized access.
5. **Promotes Good Practices**
   - Encourages strong password hygiene and reduces reuse across accounts.

2. Discussion

CRED-SAFE is a essential tool in today's digital landscape, providing a secure and efficient way to handle the increasing number of accounts and credentials. Their utility spans across individuals and organizations, offering both security and convenience. Here are the key discussion points:

1. **Importance**
   - Addresses weak and reused password practices.
   - Simplifies managing multiple credentials efficiently.
2. **Security Features**
   - Provides end-to-end encryption for secure storage.
   - Protects against attacks like phishing and data breaches.
   - Supports multi-factor authentication (MFA) for enhanced security.
3. **Usability**
   - Offers cross-platform synchronization for seamless access.
   - Features user-friendly interfaces for easy management.
4. **Limitations**
   - Dependency on the master password as a single point of failure.
   - Trust required in the provider for secure data handling.
   - Potential risk of targeted attacks on password managers.
5. **Promoting Good Practices**
   - Encourages strong password hygiene with unique and complex passwords.
   - Alerts users to data breaches for proactive account security.
6. **Future Trends**
   - Integration of biometrics for authentication.
   - Support for password less authentication systems.

7. **Conclusion**
    - Password managers enhance security and usability, making them vital tools in digital safety.

CRED-SAFE plays a crucial role in improving cybersecurity by addressing common vulnerabilities in password management. While they are not without limitations, their benefits in strengthening security, improving usability, and promoting good password hygiene make them indispensable tools in the digital age.

REFERENCES

[1] A. Adams and M.A. Sasse. Users are not the enemy. Comm. Of the ACM, 42(12):41–46, 1999

[2] R. Anderson. Why cryptosystems fail. In Proceedings of the 1st ACM Conference on Computer and Communications Security., December 1993.

[3] J.M. Carroll, P.L. Smith-Kerker, J.R. Ford, and S.A. Mazur-Rimetz. The minimal manual. Human-Computer Interaction, 3:123–153, 1987-1988.

[4] L.F. Cranor and S. Garfinkel. Security and Usability: Designing Systems that People Can Use. O'Reilly Media, edited collection edition, 2005.

[5] D. Davis. Compliance defects in public key cryptography. In Proceedings of the 6th USENIX Security Symposium, July 1996.

[6] D. Davis, F. Monrose, and M. Reiter. On user choice in graphical password schemes. In Proceedings of the 13th USENIX Security Symposium, August 2004.

[7] R. DePaula, X. Ding, P. Dourish, K. Nies, B. Pillet, D. Redmiles, J. Ren, J. Rode, and R. Silva Filho. Two experiences designing for effective security. In First Symposium on Usable Privacy and Security (SOUPS 2005), Pittsburgh, July 2005.

[8] R. Dhamija and A. Perrig. D´ej`a Vu: A User Study Using Images for Authentication. In Proceedings of the 9th USENIX Security Symposium, 2000.

[9] L. Faulkner. Beyond the five-user assumption: Benefits of increased sample sizes in usability testing. Behavior Research Methods, Instruments, & Computers, 35(3):379– 383, 2003.

[10] S.L. Garfinkel and R.C. Miller. Johnny 2: A User Test of Key Continuity Management with S/MIME and Outlook

[11] Express. In First Symposium on Usable Privacy and Security (SOUPS 2005), Pittsburgh, July 2005.