IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

KAGI – A SECURE PASSWORD MANAGER

A Zero-Knowledge & AES-256 Based Client-Side Encryption Approach

[1] Mrs Kalai Vani V, [2]Ajay Kanna A, [3]Deepan Prasath C, [4]Gokulraj S

[1]Assistant Professor, B.E CSE, [2]UG Student, B.E CSE, [3]UG Student, B.E CSE, [4]UG Student, B.E CSE
[1]Department of Computer Science and Engineering,
[1]ADHIYAMAAN COLLEGE OF ENGINEERING
(An Autonomous Institution)
Hosur, India

Abstract: The growing number of online accounts has increased the risk of weak passwords, reuse of credentials, and cyber-attacks such as phishing and identity theft. Existing password managers either lack strong security or do not fully ensure zero-knowledge privacy. This paper presents KAGI – A Secure Password Manager, designed with client-side encryption to provide complete user data confidentiality. KAGI uses AES-256-GCM encryption and PBKDF2 for secure key derivation, ensuring that passwords are accessible only to the user. The system integrates a secure password generator, multi-factor authentication, and breach monitoring using a k-anonymity model. The proposed solution enhances password security, usability, and protection against unauthorized access.

Index Terms - Password Manager, Encryption, Zero-Knowledge, AES-256, PBKDF2, Cybersecurity.

I. INTRODUCTION

The rapid growth of digital platforms has resulted in users creating and maintaining multiple online accounts across various services such as banking, social media, e-commerce, and corporate applications. This increase has led to poor password practices, including password reuse, weak credential creation, and storing passwords in unsafe mediums like notes and browsers. These unhealthy practices expose users to cyber threats such as credential theft, phishing attacks, data breaches, and unauthorized access. Existing password management approaches either depend on browser-based storage with limited security or cloud-based password managers that do not fully ensure zero-knowledge protection. To address these limitations, this study introduces KAGI – A Secure Password Manager, designed with client-side encryption, strong password generation, and multi-factor authentication to enhance data confidentiality and user privacy. The primary aim of this research is to provide a secure, user-friendly, and reliable solution for managing and protecting passwords effectively.

II. LITERATURE REVIEW

Digital security has become a growing concern due to the widespread use of online services requiring authentication. Studies indicate that weak or reused passwords contribute to a major share of cyber breaches, emphasizing the need for secure password practices. Existing password managers such as LastPass, Bitwarden, and 1Password provide encrypted vaults, but many rely on cloud-based storage, raising privacy concerns in the event of database exposure. Research on zero-knowledge systems highlights that client-side encryption ensures that service providers cannot access stored credentials, improving user privacy. Recent studies also recommend combining strong encryption with multi-factor authentication to reduce unauthorized access.

III. Research Design and Approach

This section presents the structured design and approach adopted to carry out the development of the system in a systematic and organized manner. The study followed a phased approach to ensure the design, implementation, and evaluation of the secure password manager was executed effectively. Each phase was planned to achieve the project objectives with clarity, consistency, and proper validation of results.

The project began with requirement gathering through user observation and study of existing password management challenges. Based on the identified needs, the system architecture was designed by incorporating essential security components such as AES-256 encryption, password hashing, zero-knowledge architecture, and Multi-Factor Authentication (MFA). The development approach emphasized security-focused design principles to ensure user data confidentiality and system reliability throughout usage.

After implementation, the system underwent usability and security testing to analyze performance, effectiveness, and user acceptance. The final evaluation focused on the system’s robustness, usability experience, compliance with secure coding standards, and overall ability to solve real-world password management issues. This structured research design ensured that the system was developed with a clear direction, validated outcomes, and user-centric improvements at each stage.

.

IV. RESULTS AND DISCUSSION

The results of the implemented system demonstrate that KAGI effectively enhances password security and user privacy through encryption and secure authentication methods. The use of client-side encryption ensures that password data remains inaccessible to service providers or external intruders. The password generator helps users create strong and unique passwords, significantly reducing the risk of password-related cyber-attacks. User feedback indicated that the interface is simple and easy to use, improving overall password management habits. The system’s breach-check feature also increases user awareness by notifying when stored credentials appear in known data breaches. Overall, the findings show that KAGI provides a secure, practical, and user-friendly approach to modern password management.

Abbreviation	***Full Form***
AES	Advanced Encryption Standard
MFA	Multi-Factor Authentication
KDF	Key Derivation Function
PBKDF2	Password-Based Key Derivation Function 2
GUI	Graphical User Interface
API	Application Programming Interface
UI	User Interface
OTP	One-Time Password
VPN	Virtual Private Network
SSL	Secure Socket Layer

RESEARCH METHODOLOGY

The methodology section outlines the overall plan and methods adopted for conducting this study. It explains the user population, sample selection, data sources, system framework, and architectural model used for designing the proposed secure password manager. This structured approach ensures a systematic development process, starting from requirement gathering to system design and evaluation. The details are as follows:

3.1 User Population and Sample Selection

Digital users who actively interact with multiple online platforms and require frequent authentication were considered as the population for this study. These users are more exposed to risks related to weak passwords, reuse of credentials, and cyber-attacks. The study selected a sample of 30 users, including students, working professionals, and regular internet users, to evaluate their password practices and test the developed system. These users were chosen based on the frequency of online account usage and awareness of cybersecurity practices. The selected sample assisted in analysing password behaviour, usability of the proposed system, and effectiveness of key features such as password generation, encryption, storage, and breach-alert notifications.

3.2 Data Sources and Requirements Gathering

Both primary and secondary data were used for this study. Secondary data was collected from credible cybersecurity reports, research publications, OWASP guidelines, and official encryption standard documentation to understand current password threats, encryption methods, and global security practices. Additionally, information from Have I Been Pwned (HIBP) was utilized to analyse trends in password breaches. Primary data was gathered through observation and feedback from the selected 30 users, who interacted with the system during testing. This helped in analysing usability, interface design preferences, and common password issues faced by users. The collected data facilitated the identification of key functional and security requirements essential for designing a secure password manager.

3.3 System Architecture and Security Framework

The theoretical basis of this study is founded on secure software design principles, cryptographic techniques, and zero-knowledge architecture. The dependent variable of this research is **user data security**, while independent variables include encryption strength, authentication mechanisms, and password management practices. The system follows a client-side encryption framework, where encryption and decryption operations occur locally on the user's device, ensuring that stored passwords remain inaccessible to external parties. AES-256 encryption is used for securing stored credentials, and PBKDF2 is applied for master key derivation to prevent brute-force attacks. Zero-knowledge architecture ensures that even the system provider cannot access user data. Multi-Factor Authentication (MFA) is integrated as an additional security layer to strengthen login protection. This framework aims to enhance password security, maintain privacy, and improve user trust.

3.4 Development Models and Evaluation Methods

This section describes the development model, evaluation techniques, and security methods used to transform requirements into a functional system. The methodology covers requirement analysis, development approaches, encryption models, privacy mechanisms, and system evaluation to ensure usability, security, and performance. The details are given as follows.

3.4.1 Functional and Non-Functional Requirement Analysis

Functional and non-functional requirements were identified to ensure the system meets user needs and security standards. Functional requirements include secure password storage, password generation, user authentication, breach alerts, and vault access control. Non-functional requirements address performance, usability, confidentiality, and reliability of the system. The analysis helped determine user expectations, system constraints, and security priorities. This requirement assessment also assisted in evaluating user behaviour patterns that influence password selection and management. Inputs obtained from the 30 sampled users were used to refine system functions to enhance user experience and strengthen security features. These requirements acted as the foundation for the system architecture and development design.

3.4.2 Software Development Life Cycle (SDLC) Model

The SDLC model was adopted to guide the systematic development of the secure password manager. The methodology followed phases such as requirement gathering, system design, implementation, testing, deployment, and evaluation. This model ensured that system functions were developed in a structured manner, enabling continuous improvement and validation at each stage. Documentation and feedback were maintained throughout the development cycle to ensure quality and accuracy. Testing was conducted to ensure that the system met security standards and functional expectations, with adjustments made based on results and user feedback.

3.4.2.1 Encryption Model (AES-256 and PBKDF2)

The system uses an encryption model to secure stored data. AES-256 encryption is applied to convert plaintext passwords into ciphertext to prevent unauthorized access. PBKDF2 is used for master key derivation to enhance password strength and resist brute-force attacks. The encryption model ensures that only the authorized user with the correct master password can decrypt the stored data. Proper use of salt and iteration count in PBKDF2 increases complexity, making it difficult for attackers to crack the encryption. This encryption model forms the core security layer of the password vault.

3.4.2.2 Zero-Knowledge Privacy Model

A zero-knowledge privacy model is implemented to ensure that the system provider has no access to user credentials. All encryption and decryption occur locally on the user's device, ensuring zero data exposure to external servers. Even if system data is intercepted or breached, it remains unreadable without the decryption key held by the user. The model strengthens confidentiality and aligns with modern privacy standards to build user trust. This approach ensures that users retain full ownership and control of their sensitive information.

3.4.3 Comparison of Security Approaches

The next stage of the study is to compare different security approaches to determine which technique provides better data protection and user privacy. The comparison evaluates encryption methods, authentication models, and privacy frameworks to identify the most effective approach. The study compares traditional password storage methods, basic encryption-based managers, and zero-knowledge-based systems. The effectiveness of the security approach is based on resistance to cyber-attacks, data confidentiality, and system usability.

3.4.3.1 Attack-Resistance Evaluation

This evaluation examines the resilience of the system against various cyber-attacks such as brute-force attacks, phishing, credential stuffing, and database breaches. Penetration testing and vulnerability assessments were performed to test system security. The system was found to be resistant to common attack vectors due to its strong encryption, MFA integration, and zero-knowledge architecture. The evaluation demonstrated that the implemented model enhances the security of stored credentials and reduces the risk of unauthorized access.

3.4.3.2 Performance and Security Efficiency Score

The second comparison assesses system performance and security efficiency. The evaluation considers encryption speed, authentication time, system usability, and data confidentiality. The system received a high security efficiency score based on encryption strength, low latency in operations, and user acceptance. The model ensures balance between strong security and ease of use. The findings indicate that the proposed zero-knowledge-based model is more efficient, secure, and user-friendly than traditional password management methods.

RESULTS AND DISCUSSION

4.1 Usability Evaluation of the System

This section presents the usability evaluation of the developed system, focusing on user experience, system efficiency, and ease of navigation. The evaluation aimed to determine how effectively users were able to interact with the web application and perform essential operations such as registration, login, password creation, storage, and retrieval. A total of 30 users tested the system and provided feedback based on their experience while using the platform.

Users were assigned specific tasks to perform, including creating an account, logging in using Multi-Factor Authentication (MFA), saving new passwords, viewing stored passwords, editing details, and logging out securely. Most users were able to complete these tasks successfully without external guidance. The system demonstrated smooth functionality, and users appreciated the structured layout of the interface, which made navigation easier.

The feedback received indicated that the interface was simple, responsive, and user-friendly. Users reported that the MFA-based authentication enhanced their trust in the system's security. The password generator feature was found helpful as it reduced the effort of creating strong and unique passwords manually. Overall, users expressed satisfaction with the performance of the system and found it suitable for secure password management.

Usability Factor	User Experience Summary
Interface Design	Clean, simple, and easy to understand
Navigation Flow	Smooth, clear options, and well-organized menu
Security Experience	MFA increased confidence in data protection
Learning Effort	Easy to learn, no training required
User Satisfaction	Positive feedback, users found system reliable

4.2 Security Evaluation of the System

This section presents the security evaluation of the developed system focusing on data protection, authentication strength, and resistance against common cyber threats. The purpose of this evaluation is to assess whether the system ensures confidentiality, integrity, and secure handling of user credentials. Various security measures implemented in the system were examined, including encryption, user authentication, password generation, session management, and protection against unauthorized access.

The system uses AES-256 encryption to protect stored passwords, ensuring that user credentials remain secure even if unauthorized access to the database occurs. Multi-Factor Authentication (MFA) was integrated to add an additional security layer at login, preventing entry through stolen or guessed credentials. During testing, all user accounts successfully verified authentication through a one-time verification step, and no unauthorized logins were recorded. The system was also tested against common web vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and brute-force attacks. No direct vulnerabilities were detected, and the system was able to restrict suspicious login attempts and enforce account protection features.

Furthermore, the password generator feature was evaluated for its ability to produce strong, unique, and unpredictable passwords. Users acknowledged that the automatically generated passwords improved account safety and minimized weak password usage. Secure session management ensured that user sessions expired automatically after a period of inactivity, preventing session hijacking. Overall, the security evaluation confirms that the system is robust, reliable, and provides a secure environment for managing passwords, thereby establishing user trust and safeguarding sensitive information.

V. ACKNOWLEDGMENT

I express my profound gratitude for the invaluable support and guidance I received during the execution of my Main Project at Adhiyamaan College of Engineering (An Autonomous Institution), Hosur. I sincerely thank our beloved Principal, Dr. R. Radhakrishnan, M.E., Ph.D., for providing us with the opportunity and necessary facilities to carry out this work within the college premises.

I also wish to convey my utmost respect and heartfelt thanks to Dr. G. Fathima, M.E., Ph.D., Professor and Head, Department of Computer Science and Engineering, Adhiyamaan College of Engineering (An Autonomous Institution), Hosur. Her constant guidance, valuable suggestions, and encouragement have been instrumental in the successful completion of this project.

I extend my deep gratitude to my Project Supervisor, Mrs. V. Kalai Vani, M.E., (Ph.D.), Assistant Professor, Department of Computer Science and Engineering, Adhiyamaan College of Engineering (An Autonomous Institution), Hosur, for her continuous support, insightful feedback, and motivation throughout the project, which enabled me to complete this work successfully.

I also thank the Project Coordinator and all faculty members of the Department of Computer Science and Engineering for their support, assistance, and encouragement during the course of this project.

REFERENCES

[1] J. Daemen and V. Rijmen, “Advanced Encryption Standard (AES) for Secure Data Management,” *Journal of Cryptographic Engineering*, vol. 3, no. 1, pp. 45–60, Jan. 2001.

[2] B. Kaliski, “Password-Based Key Derivation Function (PBKDF2) for Secure Key Generation,” *RSA Laboratories Technical Report*, vol. 2, no. 5, pp. 12–18, Dec. 2000.

[3] J. Broderick, “Zero-Knowledge Architecture in Password Management Systems,” *International Journal of Cybersecurity and Privacy*, vol. 8, no. 2, pp. 101–115, Mar. 2019.

[4] World Wide Web Consortium (W3C), “Web Cryptography API: Native Browser Security Implementation,” *W3C Recommendation*, vol. 1, pp. 1–25, Jan. 2017.

[5] Open Web Application Security Project (OWASP), “Guidelines for Secure Password Storage and Cryptography,” *OWASP Journal of Application Security*, vol. 4, no. 3, pp. 33–48, Jul. 2021.