myresearchgo Volume 2, Issue 5, May 2026, ISSN: 3107-3816 (Online)

Vaultix An Intelligent Zero – Knowledge Geo-Restricted Vault

[1] Atharva R. Khot, [2] Jiteshree P. Raut
[1] Student, [2] Assistant Professor

Department of Information Technology

S. D. S. M. College, Palghar, Maharashtra, India

Abstract: The increasing dependence on digital platforms has resulted in users managing numerous online accounts across banking, social media, educational portals, and enterprise systems. Consequently, password reuse, weak credential selection, and insecure storage practices have become significant cybersecurity concerns. Data breaches caused by compromised credentials continue to be among the most prevalent security incidents worldwide. Traditional password management approaches often focus solely on credential storage while overlooking aspects such as controlled sharing, user activity monitoring, and secure access management.

This research presents Vaultix, a secure credential management system designed to enhance cybersecurity through encrypted password storage, temporary access control, and comprehensive user activity monitoring. The system is developed using Angular for the frontend, Django REST Framework for the backend, and MySQL for data persistence. Vaultix employs Fernet-based cryptographic encryption to protect sensitive credentials and JWT-based authentication to ensure secure user access. The proposed architecture enables users to securely manage credentials while maintaining confidentiality, integrity, and controlled accessibility.

Furthermore, the system incorporates temporary access mechanisms that allow credential sharing with predefined expiration periods, reducing the risks associated with long-term access exposure. User activity logs provide transparency and accountability by recording critical actions performed within the platform. Through the integration of modern cybersecurity principles and secure software development practices, Vaultix offers a practical solution for mitigating credential theft, unauthorized access, and credential management challenges in modern digital environments.

Keywords: Cybersecurity, Password Management, Credential Security, Fernet Encryption, JWT Authentication, Access Control, Activity Monitoring, Vaultix

1. Introduction

The rapid growth of digital technologies has transformed the way individuals and organizations interact with online services. Users frequently access banking applications, e-commerce platforms, educational systems, cloud services, and social media accounts, each requiring secure authentication mechanisms. Passwords remain the most widely adopted authentication method despite advances in biometric and passwordless technologies.

The increasing number of digital accounts has created significant challenges in credential management. Users often resort to weak passwords, password reuse, or insecure storage methods such as notebooks, spreadsheets, or browser-based storage. These practices significantly increase vulnerability to credential theft, brute-force attacks, phishing campaigns, and account compromise.

According to multiple cybersecurity reports, compromised credentials continue to be one of the leading causes of data breaches globally. Attackers frequently exploit weak authentication practices to gain unauthorized access to sensitive information. The financial and reputational impact of such incidents has highlighted the need for secure credential management systems capable of protecting user information while maintaining usability.

Password managers have emerged as an effective solution to address these challenges. However, many existing solutions primarily focus on password storage and retrieval while providing limited support for temporary access management, activity monitoring, and controlled credential sharing. Organizations increasingly require systems that not only protect credentials but also provide accountability, visibility, and secure collaboration.

Vaultix is proposed as a cybersecurity-focused credential management platform that combines encrypted password storage, secure authentication, temporary access control, and user activity monitoring. By integrating modern cryptographic techniques and secure access management principles, Vaultix aims to provide a secure and user-friendly environment for managing sensitive credentials.

The primary objective of this research is to design and evaluate a secure credential management framework capable of reducing credential-related security risks while supporting practical usability requirements.

2. Objectives

The objectives of the project are:

- To securely store user credentials using cryptographic encryption techniques.
- To implement secure user authentication using JWT-based mechanisms.
- To provide temporary access control with configurable expiration periods.
- To improve credential security while maintaining usability.
- To establish a scalable architecture suitable for future cybersecurity enhancements.

3. Review of Literature

The rapid growth of digital services has increased the importance of secure credential management in cybersecurity. Researchers and industry standards such as NIST SP 800-63B and the OWASP Password Storage Cheat Sheet emphasize secure password handling, encryption, hashing, and the use of password managers to protect sensitive credentials.

Studies by Gasti and Rasmussen revealed that password managers may still contain vulnerabilities if cryptographic controls are poorly implemented. Modern platforms such as Bitwarden and 1Password address these concerns through end-to-end encryption and zero-knowledge architectures, reducing risks of unauthorized access.

Recent research also highlights the need for temporary credential sharing, access control, activity monitoring, and audit logging to improve accountability and detect suspicious activities. Reports from Verizon and IBM further show that compromised credentials remain a major cause of cybersecurity incidents and financial losses.

Although existing password managers provide secure storage, many lack integrated monitoring and controlled access features. The proposed Vaultix system addresses these limitations by combining encrypted credential storage, JWT-based authentication, temporary access control, and activity monitoring into a unified cybersecurity-focused credential management solution.

4. Problem Statement

The widespread use of digital services has increased the number of credentials users must manage. Traditional password storage practices expose users to security risks including password reuse, credential theft, unauthorized sharing, and account compromise**.**Existing solutions often focus on credential storage while neglecting access control and activity monitoring requirements. Consequently, users and organizations require a secure credential management system capable of protecting sensitive information while enabling controlled access and accountability.

This research aims to address these challenges through the development of Vaultix, a secure credential management platform incorporating encryption, authentication, temporary access mechanisms, and user activity monitoring.

5. Hypothesis

The increasing frequency of credential-related cyberattacks highlights the necessity for secure credential management systems that go beyond traditional password storage approaches. Existing methods often fail to provide adequate protection against credential theft, unauthorized access, and misuse of shared credentials**.** This research hypothesizes that if sensitive user credentials are protected using strong cryptographic encryption, secure authentication mechanisms, temporary access control policies, and comprehensive activity monitoring, then the risk of credential compromise, unauthorized access, and security breaches can be significantly reduced.Furthermore, it is hypothesized that integrating encrypted credential storage with expiry-based access management and user activity logging will enhance accountability, improve access governance, and strengthen the overall cybersecurity posture of credential management systems. The proposed Vaultix platform is expected to provide a secure and practical solution for managing sensitive credentials while maintaining usability and operational efficiency.

6. Limitations

Although Vaultix provides multiple security features for credential protection, certain limitations remain within the current implementation.

- The system primarily focuses on password and credential management and does not currently support multi-factor authentication (MFA), which could provide an additional layer of security.
- The encryption process is implemented using server-side cryptographic mechanisms. While secure, a true zero-knowledge architecture has not yet been implemented, meaning the server remains involved in credential processing.
- The platform currently operates as a web-based application and does not include dedicated mobile applications for Android or iOS devices.
- Temporary access management is limited to expiration-based controls and does not yet support advanced permission customization such as read-only access, approval workflows, or granular access policies.
- Activity monitoring provides visibility into user actions but does not currently incorporate automated anomaly detection or AI-based threat intelligence capabilities.
- The proposed system has been evaluated within a controlled development environment and has not undergone large-scale enterprise deployment testing.
- Cloud synchronization, disaster recovery mechanisms, and distributed key management services have not yet been integrated into the current implementation.

Despite these limitations, Vaultix establishes a strong foundation for secure credential management and provides opportunities for future cybersecurity enhancements.

7. Methodology

The development of Vaultix follows a layered architecture consisting of frontend, backend, and database components.

- **Frontend Layer:** Angular is utilized to provide a responsive and user-friendly interface. The frontend manages user interactions, form validation, authentication workflows, and credential management functionalities.
- **Backend Layer:** Django REST Framework serves as the application backend. It handles authentication, authorization, encryption processes, business logic, and activity logging.
- **Database Layer:** MySQL is used for persistent data storage. The database stores encrypted credentials, user information, access permissions, and activity logs.

The system adopts secure software development practices including input validation, secure session handling, role-based access verification, and encrypted data storage.

8. Future Scope

• Multi-Factor Authentication (MFA)

• Biometric Authentication

• WebAuthn and Passkey Integration

• AI-Based Threat Detection

• Secure File Sharing and Encryption

• Mobile Application Development

• Cloud Synchronization

• Behavioral Analytics for Anomaly Detection

• Password Breach Monitoring Services

9. Conclusion

This research presented Vaultix, a cybersecurity-oriented credential management platform designed to address contemporary credential security challenges. The system integrates cryptographic protection, secure authentication, temporary access management, and activity monitoring to provide comprehensive credential security.The implementation demonstrates that combining encryption, access control, and monitoring mechanisms can significantly improve credential protection while maintaining usability. Vaultix addresses critical cybersecurity concerns including credential theft, unauthorized access, and insecure sharing practices.The findings indicate that the proposed architecture provides a practical foundation for secure credential management and offers opportunities for future enhancements involving advanced authentication and threat detection technologies.

10. References

1. NIST Special Publication 800-63B, Digital Identity Guidelines.
2. OWASP Foundation, Password Storage Cheat Sheet.
3. Verizon Data Breach Investigations Report.
4. Django REST Framework Documentation.

5. Angular Documentation.
6. Fernet Symmetric Encryption Specification.
7. A. Gasti and K. Rasmussen, Security Analysis of Password Managers.
8. Bitwarden Security Whitepaper.
9. NIST Cybersecurity Framework.
10. CIS Critical Security Controls.