IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 5, May 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305033 |

A Review on Secure Password Manager

P. Sasi Amarnadhreddy, A. UmaShankar, Dr. A. Vijay Kumar

Department of Computer Science & Engineering, Jain (Deemed-to-be University) Bangalore, India

ABSTRACT: As the digital landscape evolves, the need for robust password management systems becomes increasingly vital. In the present research a gentle attempt is made to introduce a Secure Collaborative Password Manager, designed to address the challenges of password sharing in collaborative environments. The present research integrates advanced cryptographic techniques, distributed networking, and tokenization to ensure the utmost security and confidentiality in password transactions. In future for further enhancing the user verification it is essential to use , cross platform compactibility , user integration with enterprise systems

I. INTRODUCTION

In an era dominated by digitization, where our lives intertwine seamlessly with the digital realm, the significance of robust cybersecurity measures cannot be overstated. The proliferation of online platforms, each demanding a unique set of credentials, has given rise to the complex challenge of managing passwords securely. Recognizing this imperative need, our project endeavors to present a groundbreaking solution – the Secure Collaborative Password Manager. The Secure Collaborative Password Manager is not just a password repository; it is a sophisticated system meticulously designed to meet the demands of collaborative environments while prioritizing security. In the present research it is observed that there ia a huge gap between current pms used for sharing the credential are not so effective for sharing the credentials with other users

II. PROBLEM DEFINITION

The crux of the problem lies in the inadequacies of current systems to facilitate secure collaboration among users. In organizational settings, collaborative projects, or shared accounts, the need arises for a mechanism that allows authorized users to access shared passwords without compromising the overall security of the system. The conventional password management systems are designed with a singular user in mind, lacking the features and capabilities required for seamless and secure collaboration. One of the fundamental challenges is the absence of a standardized method for securely sharing passwords among users. In many instances, organizations resort to insecure practices such as sending passwords via unencrypted channels like email, chat, or even written documentation. Such practices expose sensitive credentials to potential breaches, as these communication channels are susceptible to interception and unauthorized access. Moreover, the current systems often lack granularity in access control when it comes to shared passwords. Collaborative projects might involve multiple stakeholders with varying levels of authority and responsibility. Existing password management systems struggle to provide a nuanced approach to permission management, leading to potential security risks. For instance, a team member requiring only temporary access to a shared account might end up having perpetual access due to the absence of dynamic permission controls.

III. LITERATURE REVIEW

The realm of password management has witnessed a surge in innovations aimed at enhancing security and collaboration. Researchers and practitioners alike have recognized the critical need for robust solutions to manage passwords securely, particularly in collaborative settings. Here, we delve into a literature review highlighting key studies and proposed models that contribute significantly to the evolution of collaborative password management. Sharma et al. delve into an Enhanced Security in Collaborative Privileged Access Management (PAM) system, incorporating multi-factor authentication and role-based access control for precise permission management. Wu et al.'s exploration of a Blockchain-Based Collaborative Password Management System introduces a tamper-proof audit trail using blockchain, smart contracts for automated permissions, and a decentralized architecture for resilience.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305033 |

Author	Title	Proposed Model	Advantages
Smith et al.	"Enhancing Collaborative Password Security"	Distributed Network with VPN, Secure Encryption	Improved collaboration, Enhanced security
Patel and Gupta	"Secure Password Management in Enterprises"	Centralized Password Manager with Multi-factor Authentication	Streamlined management, Enhanced access control
Lee and Kim	"A Review of Password Management Solutions"	Comparative analysis of existing models	Identifies strengths and weaknesses of current solutions
Wang and Zhang	"Towards a Comprehensive Password Management Framework"	Comprehensive framework integrating encryption, access controls, and audit logging	Holistic approach to password management
Chen et al.	"Design and Implementation of a Collaborative Password Manager"	Hybrid architecture combining centralized and distributed components	Balances scalability and security
Kumar and Sharma	"Security Analysis of Password Managers: A Comprehensive Review"	Evaluation of security features and vulnerabilities in password managers	Identifies potential risks and mitigation strategies
Park et al.	"User-Centric Password Management System for Mobile Devices"	Mobile-focused password management with biometric authentication	Enhanced user experience and security
González and Rodríguez	"An Analysis of Password Management Practices in Cloud Computin	Examination of password management practices in cloud environments	Highlights challenges and best practices
Li et al.	"Password Management Systems: A State-of-the-Art Review"	Overview of current trends and technologies in password management	Summarizes advancements and future directions
Huang and Chen	"A Blockchain-Based Password Management System"	Utilizes blockchain for decentralized password storage	Enhanced security and tamper-proof password storage
Liu and Wang	"Privacy-Preserving Password Management System Using Homomorphic Encryption"	Protects user privacy while managing passwords	Balances security and privacy concerns
Kim et al.	"A Novel Two-Factor Authentication Scheme for Password Management"	Introduces innovative authentication method for enhanced security	Provides additional layer of protection for user accounts
Sharma and Verma	"Biometric-Based Password Management: A Review"	Examines the integration of biometric authentication with password management	Improved security and user convenience
Wu et al.	"Machine Learning Approaches for Password Management"	Explores machine learning techniques for password management	Enhances password security through intelligent algorithms
Yang and Li	"Usability Evaluation of Password Management Interfaces"	User-centered evaluation of password management	Identifies usability issues and recommendations

IV. CONCLUSION

The Secure Collaborative Password Manager represents a significant advancement in password management systems, emphasizing both security and collaboration. The implementation integrates robust security measures, including Fernet encryption, one-time password (OTP) verification, and tokenization, ensuring that sensitive information is protected at every stage. The collaborative sharing feature sets this system apart, allowing users to securely share passwords through a distributed network while maintaining granular control over access permissions. The logging mechanism enhances transparency and accountability, providing a comprehensive history of password-sharing activities.This

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305033 |

Application addresses the limitations of traditional password managers by introducing a collaborative dimension, recognizing the evolving needs of users who often share access to various platforms. The combination of strong security features and collaborative functionality makes the Secure Collaborative Password Manager a versatile and practical solution for both individual and organizational use.

REFERENCES

[1]Adams, R.,& Sasse, M. A. (1999). Users are not the enemy.Communications of the ACM, 42(12), 40
[2]Florêncio, D., & Herley, C. (2007, May). A large-scale study of web password habits. In Proceedings of the 16th international conference on World Wide Web (pp. 657-666).
[3]El Emam, K., & Koru, G. (2008). A replicated survey of IT software project failures. IEEE software, 25(5), 84-90.
[4]Herley, C., & van Oorschot, P. C. (2009, May). A research agenda acknowledging the persistence of passwords. In Proceedings of the 2009 workshop on New security paradigms workshop (pp. 13-20).
[5]Fawaz, K., & Gellert, G. (2015, April). A survey on cryptographic approaches to secure cloud computing. In Proceedings of the 30th Annual ACM Symposium on Applied Computing (pp. 1437-1444).
[6]Bhadauria, R., Singh, A. K., & Kumar, P. (2015). A survey on cryptographic algorithms. Procedia computer science, 48, 479-485.
[7]Yee, K. P., Sitaker, J., Wiecha, C., & Malpani, A. (2000, May). The user interface for secure systems. In Proceedings of the 2000 workshop on New security paradigms (pp. 41-48).
[8]Sasse, M. A., Brostoff, S., & Weirich, D. (2001, April). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. In Proceedings of the New Security Paradigms Workshop (pp. 139-149).
[9]Dourish, P., & Anderson, K. (2006, April). Collective information practice: Exploring privacy and security as social and cultural phenomena. In Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work (pp. 321-330).
[10]Whitten, A., & Tygar, J. D. (1999, August). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In Proceedings of the 8th conference on USENIX Security Symposium (Vol. 8, p. 7).
[11]Schechter, S. E., Dhamija, R., Ozment, A., & Fischer, I. (2007). The emperor's new security indicators: An evaluation of website authentication and the effect of role-playing on usability studies. In Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP'07) (pp. 51-65).
[12]Sharp, H., Dittrich, Y., De Souza, C. R., & Eloff, J. H. (2006, May). Socio-technical systems: From design methods to systems engineering. In Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work (pp. 1-10).
[13]Gehringer, E. F., & Vegh, P. (2011). Students, passwords, and computer systems: Designing a technical intervention. Journal of Computing Sciences in Colleges, 26(6), 54-60.
[14]Liu, D., Ning, P., & Li, R. (2012). NCCloud: Applying network coding for the storage repair in a cloud-of-clouds. In IEEE INFOCOM 2012-IEEE Conference on Computer Communications (pp. 1620-1628).
[15]Kaspersky. (2021). The true value of digital privacy: Is the world standing on the brink of a privacy revolution?Retrievedfromhttps://media.kasperskydaily.com/wpcontent/uploads/sites/92/2021/04/08113918/Kaspersky_Report_The_True_Value_of_Digital_Privacy_ENG.pdf
[16]Blythe, M., & Wright, P. (2006). Paddi: designing for collaboration through digital role-play. In Proceedings of the SIGCHI conference on Human Factors in computing systems (pp. 1493-1502).
[17]Jia, X., Du, W., & Xie, J. (2009). Multi-dimensional trust computing model and its formalization. In IFIP International Information Security Conference (pp. 211-224).
[18]Gehring, S., & Helm, R. (2011). Threats to password security. Journal of Computer Information Systems, 51(4), 25-32.
[19]Cranor, L. F. (2015). Designing security and privacy tools for humans. Journal of Law and Policy for the Information Society, 11, 13-25.
[20]Fawaz, K., Gellert, G., Stojmenovic, I., & Nayak, A. (2015, April). A survey on cryptographic approaches to secure cloud computing. In Proceedings of the 30th Annual ACM Symposium on Applied Computing (pp. 1437-1444)

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details