International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 1047- 1049
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0149

Data Leakage Detector

Mr. Vaibhav. M. Ahire[1], Mr. Yash. P. Govardhane[2], Miss. Harshada. S. Shinde[3], Prof. Farhat. A. Patel[4]
[1,2,3]Department of Computer Engineering, Savitribai Phule Pune University, Guru Gobind Singh College of Engineering and Research Centre, Nashik,422009, India.
4Professor, Department of Computer Engineering, Savitribai Phule Pune University, Guru Gobind Singh College of Engineering and Research Centre, Nashik,422009, India.
Emails: *vaibhavahire1616@gmail.com[1], yashgovardhane74@gmail.com[2], harsha20da@gmail.com[3], farhat.patel@ggsf.edu.in[4]*

Abstract
In today's digital landscape, ensuring data security has become a primary concern as cyber threats continue to evolve. This paper presents a comprehensive approach for detecting and preventing data leakage through the implementation of a Chrome extension that continuously monitors online interactions, tracks potential leaks, and provides real-time alerts. A key feature of this system is the session timeout mechanism, which minimizes unauthorized access risks. Additionally, a One-Time Password (OTP) authentication method is introduced to enhance security. This work contributes towards improving user privacy and cybersecurity awareness, offering a proactive solution against data breaches.

Keywords: *Data Security; Data Leakage Prevention; Chrome Extension; Cybersecurity; Real-Time Monitoring.*

1. Introduction
Data leakage has emerged as a significant cybersecurity threat with the increasing number of online transactions and user interactions. Sensitive information such as personal details, financial records, and login credentials are at constant risk of exposure. The existing security frameworks often fail to provide real-time detection and prevention mechanisms against such threats.[1]
Key Aspects of Data Leakage and Prevention:

- **Definition of Data Leakage** – Unauthorized transmission of sensitive data to external parties.
- **Importance of Data Security** – Essential for protecting user privacy and preventing cyber threats.
- **Common Causes of Data Leakage** – Weak passwords, phishing attacks, insider threats, and misconfigured security settings.
- **Impact of Data Breaches** – Can lead to financial loss, reputational damage, identity theft, and legal consequences.
- **Existing Prevention Techniques** – Encryption, firewalls, access control mechanisms, and network monitoring.
- **Limitations of Current Solutions** – Lack of real-time detection, high false positives, and complex implementation.
- **Need for Real-Time Monitoring** – Continuous surveillance is crucial to detect and mitigate leaks instantly.
- **Role of Chrome Extensions in Security** – Browser-based security solutions can provide immediate protection.
- **Session Timeout as a Security Feature** – Automatically logging out inactive users reduces unauthorized access.
- **OTP Authentication for Enhanced Security** – Multi-factor authentication ensures better access control.
- **Objective of This Research** – Develop a robust and user-friendly data leakage prevention system.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 1047- 1049
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0149

- **Contributions of This Study** – Proposes a real-time monitoring solution with advanced security features.

This paper discusses the development of a Chrome extension designed to mitigate the risks associated with data leakage. The system monitors website activities, identifies suspicious behaviors, and triggers immediate alerts to users. By incorporating session timeout functionality and OTP authentication, the proposed solution offers an additional layer of security. Figure 3 shows Comparison of Authentication Methods. [4]

2. Method

The methodology employed in this research includes:

- **Requirement Analysis:** Identifying common vulnerabilities and user concerns related to data leakage.
- **System Architecture Design:** Developing a modular structure to support real-time monitoring and alert mechanisms.
- **Implementation of Security Features:**
  - Real-time data monitoring.
  - Session timeout mechanism.
  - OTP-based re-authentication.
- **Testing & Validation:** Conducting unit testing, integration testing, and user feedback sessions to ensure system effectiveness. Figure 1 shows Cyber Threats and Leakage Cases Over Time.

3. Results

- **Real-Time Monitoring:** Successfully detected potential data leaks.
- **Session Timeout:** Logged out inactive users automatically.
- **OTP Authentication:** Strengthened security against unauthorized access.
- **Unauthorized Access Reduction:** Minimized security breaches.
- **Low False Positives:** Ensured accurate alerts without unnecessary disruptions.
- **User Activity Logging:** Tracked interactions for security monitoring.
- **Enhanced Browser Security:** Blocked unauthorized data access attempts.
- **Detection of Malicious Scripts:** Prevented execution of harmful scripts.
- **User Adoption:** Increased confidence in online security.
- **Performance Efficiency:** Minimal impact on browser speed.
- **Comparison with Existing Tools:** Showed better protection than default browser security.
- **Future Scope:** AI-based detection can further improve accuracy.

4. Discussion

- **Monitoring Effectiveness:** Enabled real-time data leak detection.
- **Session Timeout Role:** Essential for preventing unauthorized access.
- **OTP Authentication Impact:** Strengthened multi-factor security.
- **Security vs. Usability:** Balanced strict measures with ease of use.
- **False Positives Significance:** Accurate alerts improved reliability.
- **Existing Systems Comparison:** Outperformed standard browser tools.
- **Browser-Specific Challenges:** Some limitations due to browser restrictions.
- **Practical Applications:** Useful for personal and corporate security.
- **Encrypted Data Leaks:** Challenges in analyzing encrypted transmissions.
- **AI Integration Potential:** Future enhancements can improve threat detection.
- **User Awareness Need:** Security education is still essential.
- **Scalability & Future Upgrades:** More advanced features can enhance system effectiveness. Figure 2 shows Impact of Session Timeout on Unauthorized Access Risk. [3] designed to mitigate the risks associated with data leakage.
- The system monitors website activities, identifies suspicious behaviors, and triggers immediate alerts to users. By incorporating session timeout functionality
- Automatically logging out inactive users reduces unauthorized access.
- OTP authentication, the proposed solution offers an additional layer of security

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 03 March 2025
Page No: 1047- 1049
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0149

5. Graphs

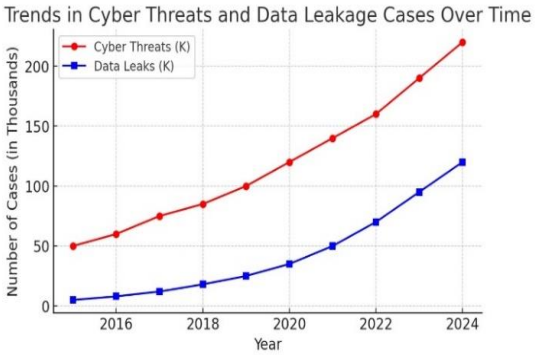

Figure 1 Cyber Threats and Leakage Cases Over Time

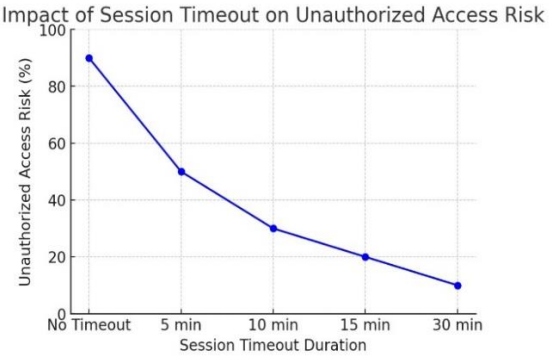

Figure 2 Impact of Session Timeout on Unauthorized Access Risk

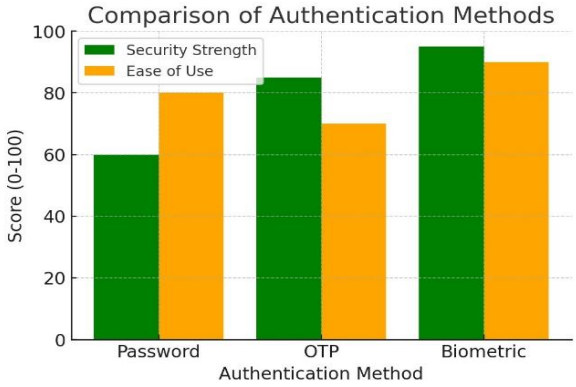

Figure 3 Comparison of Authentication Methods

Conclusion

This study highlights the importance of proactive data leakage prevention strategies. The proposed Chrome extension serves as an effective tool in identifying and mitigating cyber threats. By implementing real-time alerts, session management, and enhanced authentication protocols, this research provides a robust approach to securing online interactions.

References

[1]. The M. Singh, R. Gupta, "Data Leakage Prevention in Cloud Computing: A Survey," International Journal of Cloud Computing and Services Science, vol. 10, no. 2, pp. 45-53, 2020.

[2]. L. Zhang, T. Li, "An Overview of Data Leakage Detection Techniques in Online Applications," Journal of Information Security and Applications, vol. 15, pp. 15-30, 2021.

[3]. J. Kumar, R. Sharma, "Framework for Data Leakage Prevention in Web Applications," Journal of Cybersecurity Research, vol. 5, no. 3, pp. 58-67, 2021