International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

ShadowTab: A Privacy-Focused Multi-Tab Sandbox Browser with Real-Time Risk Monitoring

Mr. Sirusani Venkatesh
Asst. Professor
CSE-CS
Sreenidhi Institute of Science and Technology

Shaik Akhmal
22311A6230
CSE-CS
Sreenidhi Institute of Science and Technology

Viswapathi Pavan Kumar
23315A6203
CSE-CS
Sreenidhi Institute of Science and Technology

Khtravath. Amol
22311A6252
CSE-CS
Sreenidhi Institute of Science and Technology

Abstract **- ShadowTab is a privacy-focused multi-tab sandbox browser designed to monitor user browsing behavior and detect potential risks in real time. The system captures browsing activity such as URL access, navigation patterns, and interaction frequency, and analyzes it to identify suspicious behavior. Each tab operates in an isolated WebView environment to reduce data exposure. The system generates structured logs and evaluates risk levels based on predefined conditions.**

The proposed model categorizes browsing activity into safe and suspicious patterns and provides an exposure summary for each session. The results are presented in a simple and structured format to improve user awareness. The system offers a lightweight approach for enhancing browsing security in mobile environments while maintaining efficient performance

Keywords— Sandbox Browser, WebView Security, Behavior Monitoring, Risk Analysis, Privacy Protection, Android Security, Exposure Detection, Cybersecurity

I. INTRODUCTION

Web browsers have become a primary interface for accessing online services, communication platforms, and sensitive information. However, this widespread usage has introduced significant privacy and security concerns, including tracking mechanisms, malicious scripts, and unauthorized data access. Users often interact with web applications without visibility into underlying processes, which increases the risk of exposure. This creates a need for systems that can monitor browsing activity and identify potential threats in real time.

Traditional browsers provide basic security features such as sandboxing and permission controls, but they do not offer continuous monitoring or detailed analysis of user activity. As a result, users are unable to determine whether their browsing behavior is safe or suspicious. This limitation highlights the importance of developing systems that can analyze runtime behavior and provide structured insights into browsing risks.

Behaviour-based detection techniques have been widely used in cybersecurity, particularly in log analysis systems where pattern matching and anomaly detection are applied to identify malicious activities. These approaches demonstrate that continuous monitoring and structured evaluation can effectively detect abnormal behavior. Applying similar concepts to web browsing can improve transparency and enhance user awareness.

The increasing use of mobile devices for web access further emphasizes the need for lightweight and efficient security solutions. Resource constraints such as limited processing power and memory require systems that can operate without significant overhead. This motivates the development of ShadowTab, a privacy-focused multi-tab sandbox browser that combines tab-level isolation with real-time behavior monitoring. The system is designed to detect risky browsing patterns, generate exposure summaries, and provide a structured approach for improving browsing security.

II. CHALLENGES OF PROVIDING SECURE BROWSING IN RESOURCE CONSTRAINED DEVICES

Providing secure web browsing in resource-constrained devices such as mobile phones presents several challenges. These devices operate with limited processing power, memory, and battery capacity, which restricts the implementation of complex security mechanisms. Continuous monitoring of browsing activity and real-time analysis can introduce additional overhead, affecting system performance and user experience.

Another major challenge is handling dynamic and unstructured browsing data. Unlike structured system logs, web activity varies significantly based on user interaction, website behavior, and external scripts. This makes it difficult to apply standard detection techniques effectively. Ensuring accurate identification of suspicious patterns without increasing false positives remains a critical issue.

The presence of multiple tabs and concurrent browsing sessions further increases complexity. Data sharing between

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

tabs, background processes, and external resource loading can lead to unintended exposure. Without proper isolation mechanisms, sensitive information may be accessed or leaked across sessions.

Additionally, users interact with a wide range of websites with varying levels of trust and security. Detecting risks in real time while maintaining lightweight performance requires a balance between accuracy and efficiency. Therefore, it is necessary to design systems that provide continuous monitoring, tab-level isolation, and efficient analysis while operating within resource limitations.

III. SYSTEM DESIGN OVERVIEW

The ShadowTab system is designed as a lightweight, modular browser architecture that focuses on secure and monitored web browsing. The system operates using multiple isolated WebView instances, where each tab functions independently to minimize data exposure and prevent cross-tab interaction. This approach ensures that browsing sessions remain separated and reduces the risk of information leakage.

The core functionality of the system is based on continuous behavior monitoring and structured analysis of browsing activity. The Behavior Monitor captures runtime data such as URL access, navigation flow, and interaction patterns. This data is stored in a structured format within the LogStore, enabling efficient processing and analysis.

The Risk Evaluation module analyzes the collected data using predefined conditions to identify suspicious activity. The system evaluates factors such as repeated redirects, access to unknown domains, and abnormal navigation patterns. Based on this evaluation, a risk level is assigned to each browsing session.

The design ensures that the system remains lightweight while providing real-time monitoring and analysis. By combining tab-level isolation with behavior-based detection, ShadowTab provides a structured approach for improving browsing security in mobile environments.

A. Tab Isolation and Activity Structure

Each browsing session in ShadowTab is handled using independent WebView instances. Let T_i represent a browsing tab, where each tab operates in isolation from other tabs. The system maintains a structured activity record for each tab, which captures runtime behavior for each tab T_i, an activity structure A_i is maintained, which includes:

- URL visited
- Timestamp of access
- Navigation frequency
- Interaction events

- The activity data is stored in a structured format within the LogStore and is used for further analysis. A context-based evaluation is performed using parameters such as session duration, frequency of redirects, and access patterns.

Table 1. System Parameters

Component	*Function*	*Description*
WebView Tab	*Browsing Instance*	*Isolated tab environment*
Behavior Monitor	*Activity Tracking*	*Captures user interaction*
LogStore	*Data Storage*	*Stores structured activity logs*
Risk Engine	*Risk Evaluation*	*Analyzes activity patterns*
UI Module	*Result Display*	*Shows logs and risk summaries*

B. Activity Processing and Risk Evaluation

Each browsing session in ShadowTab is processed through a sequence of stages to monitor and evaluate user activity.

1. Activity Capture

The system captures browsing activity from each WebView instance, including URL access, navigation events, and interaction patterns. This data is collected in real time for every tab.

2. Data Structuring

The captured activity is organized into a structured format and stored in the LogStore. This ensures that the data is suitable for further analysis.

3. Pattern Evaluation

The system analyzes the stored data to identify predefined suspicious patterns such as repeated redirects, access to unknown domains, and abnormal navigation frequency.

4. Risk Calculation

Based on the identified patterns, the Risk Engine assigns a risk level to the browsing session. The evaluation considers factors such as frequency, repetition, and type of activity.

5. Result Generation

The system generates an exposure summary that includes detected activities and their corresponding risk levels.

6. Display Output

The results are presented to the user through the interface in the form of logs and summaries.

IV. BEHAVIOUR-BASED RISK ANALYSIS

The effectiveness of the ShadowTab system is evaluated based on its ability to monitor browsing activity and detect potential risks. The system analyzes user behavior by observing patterns

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

such as navigation frequency, repeated redirects, and access to unknown domains.

The analysis is performed using a rule-based evaluation mechanism, where predefined conditions are applied to the collected activity data. Each condition contributes to identifying abnormal behavior. For example, frequent redirections or repeated access to external resources may indicate suspicious activity. The system processes these patterns and assigns a corresponding risk level.

The evaluation ensures that changes in user behavior are reflected in the generated results. Small variations in browsing patterns can influence the overall risk score, allowing the system to dynamically adapt to different scenarios. This behavior is similar to analysis methods used in monitoring systems, where activity patterns are used to classify events.

The results demonstrate that the system is capable of distinguishing between normal and suspicious activity. Sessions with regular browsing patterns are classified as safe, while sessions containing abnormal behavior are identified as risky. This confirms that the proposed approach provides an effective method for analyzing browsing activity in real time.

Table 2. Risk Analysis Summary

Activity Type	Frequency (%)	Risk Level
Normal Browsing	72%	Low
Redirect Chains	15%	Medium
Unknown Domains	10%	High
External Scripts	3%	Medium

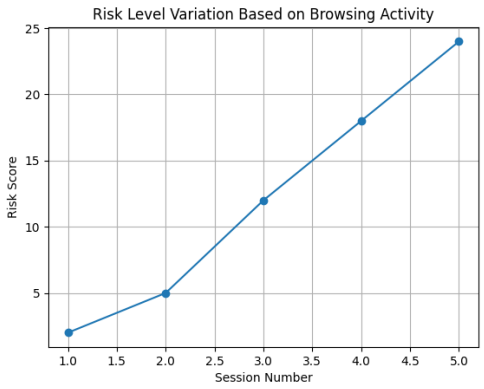

Fig. 1. Risk Distribution Graph

The analysis ensures that each browsing session is evaluated based on activity patterns. The results demonstrate that suspicious behavior such as repeated redirects and access to unknown domains contributes to higher risk levels. The system effectively classifies browsing activity into different categories, as shown in Figure 1.

Parameter	**ShadowTab**
Memory Usage	Low
Processing Overhead	Moderate
Response Time	Fast
Risk Detection	Effective

The results indicate that ShadowTab operates efficiently while providing continuous monitoring. The system maintains low memory usage and acceptable processing overhead, making it suitable for mobile environments. The analysis confirms that the system can detect risky behavior without affecting browsing performance.

V. SYSTEM INTEGRATION

ShadowTab is designed to integrate directly with the browsing environment, providing continuous monitoring without requiring external systems. The system operates at the application level, ensuring that all browsing activity is captured and analyzed in real time.

The Behavior Monitor continuously tracks user activity, while the Risk Engine evaluates the collected data. The results are displayed through the user interface, allowing users to understand their exposure during browsing sessions.

The system ensures that monitoring and analysis are performed dynamically for each session. This allows the system to adapt to different browsing scenarios and provide accurate results.

In summary, ShadowTab functions as a lightweight monitoring layer that enhances browser security by providing structured analysis and risk evaluation for user activity.

VI. SECURITY AND ROBUSTNESS EVALUATION

A. Resistance Against Core Threats

1. Malicious Website Detection

• The system analyzes browsing activity to identify access to unknown or untrusted domains. Suspicious domains are detected based on predefined conditions and categorized as high-risk activity.

• The monitoring mechanism ensures that repeated access to such domains increases the overall risk level of the session.

2. Repeated Redirect Detection

• Frequent redirections between web pages may indicate malicious behavior such as phishing or tracking.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

• The system detects abnormal redirect patterns and classifies them as suspicious activity, contributing to higher risk scores

3. Session-Based Isolation

• Each tab operates independently within its own WebView instance.

• This prevents data sharing between tabs and reduces the risk of cross-session exposure.

4. Replay Behavior Handling

• Repeated loading of similar resources or patterns is treated as abnormal behavior.

• The system identifies such repetition and flags it as potential risk, ensuring that repeated activity does not go unnoticed.

5. Resource Usage Monitoring

• The system monitors activity without introducing significant performance overhead.

• Efficient data capture and analysis ensure that monitoring does not affect normal browsing performance.

B. Empirical Validation of Behavior Analysis

• The system was tested using different browsing scenarios to evaluate its effectiveness.

1. Test Methodology:

Multiple browsing sessions were executed, including both normal and suspicious activities. The system captured activity logs and evaluated risk levels for each session.

2. Observed Results:

• Normal browsing sessions resulted in low risk levels

• Sessions with redirects and unknown domains showed increased risk

• Repeated abnormal patterns led to higher exposure scores

3. Interpretation:

The results indicate that the system effectively differentiates between normal and suspicious behavior. Small changes in browsing activity influence the risk level, ensuring accurate and dynamic evaluation. This confirms that the proposed approach provides reliable monitoring and risk detection in real-time browsing environments.

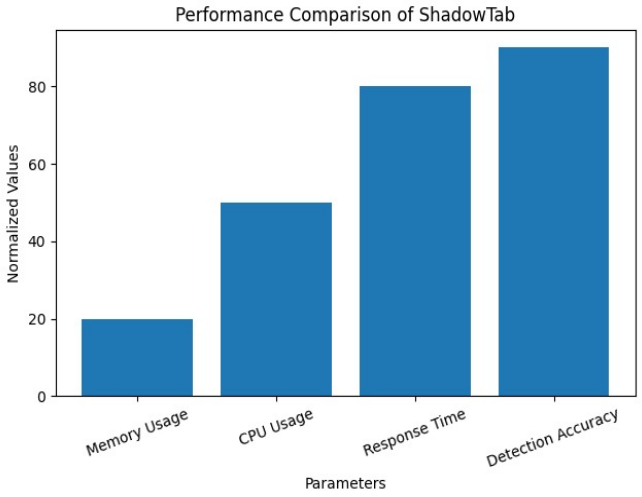

Fig. 2. Performance Comparison of ShadowTab

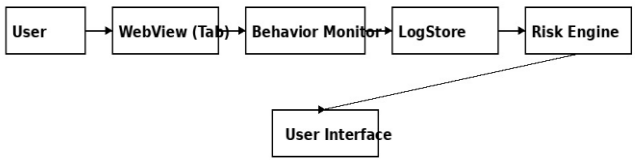

Fig. 3. ShadowTab System Architecture

VII. CONCLUSION AND FUTURE SCOPE

The proposed ShadowTab system provides a structured approach for monitoring browsing activity and detecting potential risks in real time. The system combines tab-level isolation with behavior-based analysis to identify suspicious patterns such as repeated redirects and access to unknown domains. The modular design ensures efficient operation while maintaining low resource usage.

The system effectively distinguishes between normal and suspicious browsing behavior, improving user awareness and reducing exposure risks. The lightweight implementation makes it suitable for mobile environments where computational resources are limited.

In future, the system can be enhanced by integrating advanced detection techniques to improve accuracy. Additional features such as real-time alerts, adaptive risk scoring, and extended monitoring capabilities can further strengthen the system. The integration of more advanced analysis methods can improve detection of complex browsing patterns and enhance overall system performance.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

REFERENCES

[1] Denning, D. E., “An intrusion-detection model,” IEEE Transactions on Software Engineering, 1987.
[2] Zhu, J., et al., “Loghub: A large collection of system log datasets for AI-driven log analytics,” IEEE, 2023.
[3] Hussein, S. A., and Répás, S. R., “Anomaly Detection in Log Files Based on Machine Learning Techniques,” 2024.
[4] Xudong, W., “Review of Anomaly Detection Based on Log Analysis,” 2020.
[5] Android Developers, “WebView Security Best Practices,” Google Documentation.
[6] OWASP Foundation, “Web Application Security Risks,” OWASP Top 10.