International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 14, Issue 1, 2026

Real-Time Web Page Malware Detection

Suddala Vishal[1], Mrs. M.Anusha[2]
B.Tech Student, Department Of Electronics and Computer Engineering, J.B Institute of Engineering and Technology, Hyderabad, India[1]
Assistant Professor, Department Of Electronics and Computer Engineering, J.B Institute of Engineering and Technology, Hyderabad, India[2]
vishalsuddala24@gmail.com, anusha.ecm@jbiet.edu.in

ABSTRACT

Real-time mobile web page malware detection is essential for safeguarding users from online threats. With the rapid growth of mobile browsing, malicious web pages have become a major security concern. This approach detects malware instantly as users access web pages through their mobile devices. It uses lightweight machine learning algorithms to analyze webpage content, scripts, and behavior. Features such as URL structure, embedded JavaScript, and external links are evaluated. Real-time detection ensures immediate blocking of harmful sites, minimizing user risk. Cloud-based scanning and on device filters enhance performance and scalability. The system updates threat databases continuously for evolving attacks. It avoids delays or excessive battery consumption, making it suitable for mobile use.

Privacy preserving techniques are integrated to protect user data. This method strengthens overall mobile cybersecurity. It offers a fast, efficient, and effective solution against web-based malware threats.

Introduction

Real-time mobile web page malware detection is an essential security mechanism aimed at identifying and mitigating the risks associated with malicious activities targeting mobile users. With the rise in mobile internet usage, attackers have increasingly targeted mobile web applications, exploiting vulnerabilities in both websites and the underlying devices. The need for real-time detection systems stems from the growing volume of mobile malware attacks, which can cause data theft, privacy violations, and financial losses. Real-time detection allows immediate identification and mitigation of potential threats, ensuring user protection and maintaining the integrity of mobile web applications.

The mobile web has become a primary source of online interactions, enabling users to access a wide range of services, from banking to social networking. However, the convenience of mobile browsing comes with significant security risks. Malicious actors have devised sophisticated strategies, such as phishing, JavaScript-based exploits, and drive-by downloads, to compromise users' devices and data. Consequently, mobile malware detection is critical to secure the browsing experience. Real-time detection systems work by analyzing web pages in real time, scanning for known and unknown threats, and providing an active defense against malicious content.

Real-time detection of mobile web page malware often involves the use of heuristic-based approaches, signature-based systems, and machine learning algorithms. Heuristic methods help identify potentially dangerous behaviors and code patterns, while signature-based systems match known malware signatures against the web content. However, these approaches alone are not sufficient, as malware developers continuously adapt to evade detection. Machine learningbased solutions offer promising advancements by dynamically learning from emerging threats, improving the accuracy of malware detection, and reducing false positives. By integrating these techniques, real-time detection systems provide a more robust solution to combat the evolving nature of mobile web threats.

In addition to detecting threats, real-time mobile web page malware detection plays a key role in protecting users' privacy and sensitive data. Privacy breaches resulting from malware infections can expose personal information such as passwords, credit card numbers, and other confidential data. Real-time detection systems aim to identify malicious web pages before they can compromise users' data. By employing techniques like sandboxing, behavior analysis, and URL filtering, these systems ensure that any detected threats are neutralized before they can execute on users' devices, thereby safeguarding privacy.

The challenge of real-time malware detection on mobile web pages also lies in balancing security with user experience. Intrusive security measures can degrade performance, leading to slower web browsing and reduced user satisfaction. As a result, it is vital for detection systems to operate seamlessly, without significantly affecting the user experience. This balance is crucial for the

widespread adoption of malware detection tools and their effectiveness in the real-time protection of mobile users. Achieving this requires efficient algorithms, optimized scanning processes, and continuous updates to stay ahead of the constantly evolving malware landscape.

Problem Statement

The increasing prevalence of mobile web browsing has made mobile devices prime targets for cybercriminals, leading to a rise in malware attacks specifically designed to exploit vulnerabilities in mobile web pages. These attacks, which can include phishing, data theft, and malicious code execution, threaten the privacy, security, and financial well-being of mobile users. Despite the availability of various security measures, existing solutions often fail to provide real-time detection and mitigation, leaving users vulnerable to emerging threats. The challenge lies in developing an effective real-time malware detection system that can promptly identify and neutralize malicious web pages without compromising user experience. This research aims to address the gaps in current security approaches by designing and implementing a robust real-time detection mechanism that can accurately identify mobile web page malware, adapt to new threats, and operate seamlessly on mobile devices.

Literature Survey

Title: A Survey on Mobile Web Malware Detection Techniques
Authors: R. Sharma, M. Kumar, and S. Agarwal
Year: 2015
Abstract: This paper provides an in-depth survey of various mobile web malware detection techniques, with a focus on real-time analysis for enhancing mobile security. The authors explore different methods employed to detect malicious web pages targeting mobile devices, such as static and dynamic analysis, machine learning algorithms, and heuristic-based approaches. By analyzing the limitations and strengths of each technique, the paper discusses how real-time detection can be integrated into mobile browsers and apps to protect users from malicious content. The study also highlights the challenges posed by rapidly evolving attack vectors and the need for more adaptive, context-aware security solutions. The paper concludes by emphasizing the importance of combining multiple detection techniques to ensure effective and scalable mobile web malware protection.

Title: Real-Time Detection of Web-Based Malware Attacks on Mobile
Devices Using Machine Learning
Authors: A. Mehta, P. Jain, and S. Roy
Year: 2016
Abstract: This research investigates the application of machine learning techniques for real-time mobile web page malware detection. The authors propose a novel framework that uses classification algorithms such as decision trees and support vector machines (SVM) to detect malicious mobile web pages in real-time. By extracting features from URLs, page content, and web traffic patterns, the proposed model can accurately classify web pages as benign or malicious. The paper demonstrates the effectiveness of the framework through extensive experiments on real-world datasets, showing a significant improvement in detection accuracy and processing speed compared to traditional methods. This study highlights the potential of machine learning to enhance the efficiency and scalability of mobile web malware detection systems.

Title: Hybrid Malware Detection System for Mobile Web Pages: Real-
Time Malware Classification
Authors: R. Patel, K. Joshi, and T. Sharma
Year: 2017
Abstract: This paper introduces a hybrid malware detection system for mobile web pages, combining both static and dynamic analysis to detect malicious behavior in real-time. The authors propose a system that analyzes web page source code (static analysis) and monitors the behavior of scripts executed on mobile browsers (dynamic analysis) to detect malicious activity. By leveraging both approaches, the system provides a more comprehensive solution for identifying sophisticated malware that evades traditional detection methods. The research demonstrates the effectiveness of this hybrid system on a variety of malware samples, achieving high detection rates with low falsepositive rates. The paper also discusses the challenges involved in real-time malware detection, such as the need for low computational overhead and minimal impact on user experience.

Title: Real-Time Malware Detection in Mobile Web Pages Using Behavior Analysis
Authors: M. Singh, N. Rani, and S. Kapoor
Year: 2018
Abstract: This paper explores the use of behavior analysis for realtime malware detection on mobile web pages. The authors focus on detecting malware by analyzing the behavior of web pages, such as page redirects, pop-ups, and unusual script activities that may indicate malicious intent. The study employs a monitoring tool that tracks web page interactions on mobile browsers and compares them to known patterns of benign and malicious behavior. The authors introduce a novel approach that combines real-time behavior analysis with a database of threat signatures to detect new and

evolving webbased malware. Through experiments, the paper demonstrates that this approach provides an effective and low-latency solution for realtime mobile web malware detection, capable of identifying threats in seconds.

Title: Deep Learning-Based Real-Time Mobile Web Page Malware Detection
Authors: V. Gupta, S. Joshi, and M. Agarwal
Year: 2019
Abstract: In this paper, the authors apply deep learning techniques to real-time mobile web page malware detection. The proposed system leverages Convolutional Neural Networks (CNNs) to automatically learn features from mobile web pages, such as HTML structure, URL patterns, and embedded scripts, for detecting malicious behavior. By using a large dataset of labeled web pages, the system trains a deep learning model to classify web pages as either safe or malicious. The authors show that deep learning significantly outperforms traditional rule-based and machine learning approaches, offering higher accuracy in detecting novel malware. The paper also discusses the challenges of implementing deep learning models in mobile environments, including the need for efficient computational resources and fast processing times to ensure a seamless user experience.

Title: Anomaly-Based Detection for Mobile Web Malware: Real-Time
Detection System
Authors: A. Thakur, R. Gupta, and P. Jain
Year: 2020
Abstract: This paper focuses on anomaly-based detection methods for real-time mobile web malware detection. The authors propose an anomaly detection system that continuously monitors mobile web page activities, such as network traffic, API calls, and data requests, to identify unusual patterns indicative of malicious behavior. By using machine learning algorithms to establish a baseline of normal behavior, the system can identify deviations that may suggest an attack. The paper presents experimental results that show the efficacy of the anomaly-based approach in detecting zero-day malware attacks and novel web-based threats. The study emphasizes the importance of real-time anomaly detection in enhancing mobile web security and discusses the potential challenges in terms of false positives and the system's ability to scale across different devices.

Title: Real-Time Malware Detection for Mobile Web Pages Using URL
Analysis and Behavioral Features
Authors: N. Kumar, R. Rathi, and S. Mehta
Year: 2021 **Abstract:**
In this study, the authors introduce a real-time mobile web page malware detection system that utilizes URL analysis combined with behavioral features. The system analyzes web page URLs for patterns commonly associated with malicious sites and cross-references them with known blacklists. Additionally, the system monitors the behavior of web page scripts and network traffic to identify potential threats in real-time. The paper demonstrates that this combined approach significantly improves the detection accuracy by considering both static and dynamic features of web pages. The authors present experimental results showing the system's ability to detect a wide range of mobile web malware, including phishing, drive-by downloads, and adware, with low latency and minimal computational overhead.

Title: A Lightweight Real-Time Mobile Web Malware Detection System for Resource-Constrained Devices
Authors: S. Thakur, M. Kapoor, and N. Sharma
Year: 2022
Abstract: This paper addresses the challenge of real-time mobile web malware detection on resource-constrained devices. The authors propose a lightweight detection system that balances accuracy with computational efficiency, making it suitable for smartphones and tablets with limited processing power. The system uses a combination of heuristic-based techniques and lightweight machine learning models to detect mobile web page malware in real-time. The authors evaluate the system on several mobile devices, showing that it maintains high detection accuracy without significantly affecting device performance. This research is particularly relevant for mobile security in developing regions, where smartphones are widely used but often lack high-end hardware capabilities.

Title: Real-Time Mobile Web Malware Detection Using Hybrid Deep
Learning and Heuristic Techniques
Authors: R. Sharma, A. Jain, and S. Sood
Year: 2023
Abstract: This paper proposes a hybrid approach for real-time mobile web malware detection that combines deep learning techniques with heuristic methods. The authors argue that while deep learning excels at identifying complex patterns in web page content, heuristic techniques can effectively detect known malware patterns with minimal computational overhead. By integrating both approaches, the proposed system provides fast, accurate, and scalable malware detection for mobile web pages. The authors present experimental results showing that the hybrid system outperforms traditional methods in terms of detection accuracy and response time, making it suitable for real-time

mobile security applications. This study also addresses the challenges of handling evolving malware threats and the need for continuous model updates.

Title: The Evolution of Real-Time Malware Detection on Mobile Web Pages: Challenges and Future Directions
Authors: M. Singh, R. Yadav, and N. Kapoor
Year: 2024
Abstract: This paper provides a comprehensive review of the evolution of real-time malware detection techniques for mobile web pages, with a particular focus on challenges faced in developing effective detection systems. The authors review previous studies, outlining the progression from basic heuristic methods to advanced machine learning and deep learning-based systems. They also identify key challenges in real-time malware detection, including handling largescale data, minimizing false positives, and ensuring fast detection times without compromising accuracy. The paper concludes with a discussion of future research directions, including the use of federated learning and decentralized detection systems, which could further enhance the security and scalability of real-time mobile web malware detection.

System Analysis

Existing System

Existing systems for real-time mobile web page malware detection primarily rely on traditional methods such as signature-based detection, heuristic analysis, and URL filtering. Signature-based detection involves matching known malware signatures with the content of web pages, while heuristic methods identify suspicious patterns or behaviors. URL filtering blocks known malicious websites based on blacklists. Although these approaches can effectively identify some threats, they are limited in scope, often failing to detect new or evolving malware strains that do not match predefined signatures. Additionally, these systems can be slow, leading to delays in threat detection and potentially compromising the user experience. Recently, machine learning and artificial intelligence have been integrated into some detection systems, offering more dynamic and adaptive solutions. These systems learn from past malware attacks, enabling them to predict and identify unknown threats more accurately. However, despite advancements, many existing systems still struggle with balancing real-time detection with minimal performance impact on mobile devices, as well as handling the sheer volume of web traffic and the complexity of modern web-based threats. Therefore, there is a need for more advanced, efficient, and adaptive solutions that can provide faster and more comprehensive malware detection for mobile web pages in real-time.

Proposed System

The proposed system for real-time mobile web page malware detection aims to address the limitations of existing solutions by integrating advanced techniques such as machine learning, behavioral analysis, and dynamic threat modeling. Unlike traditional signature-based systems, this approach focuses on detecting both known and unknown threats by analyzing the behavior of web pages in real-time. Machine learning algorithms will be trained to identify malicious patterns, such as unusual network activity, JavaScript exploitation, and suspicious content, without relying solely on predefined signatures. The system will dynamically adapt to new malware variants, improving its detection capabilities as it learns from emerging threats. Additionally, the proposed system will incorporate lightweight scanning techniques to minimize the impact on mobile device performance, ensuring seamless browsing experiences while providing robust security. The real-time detection framework will also include a proactive alert mechanism, notifying users instantly when a threat is detected, and blocking malicious web pages before they can execute harmful actions, such as data theft or device infection. This system will provide a more comprehensive, efficient, and adaptive solution for mobile web page malware detection, offering enhanced protection without compromising user experience or device resources.

System Design

Data Flow Diagram:

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 14, Issue 1, 2026

System Architecture:

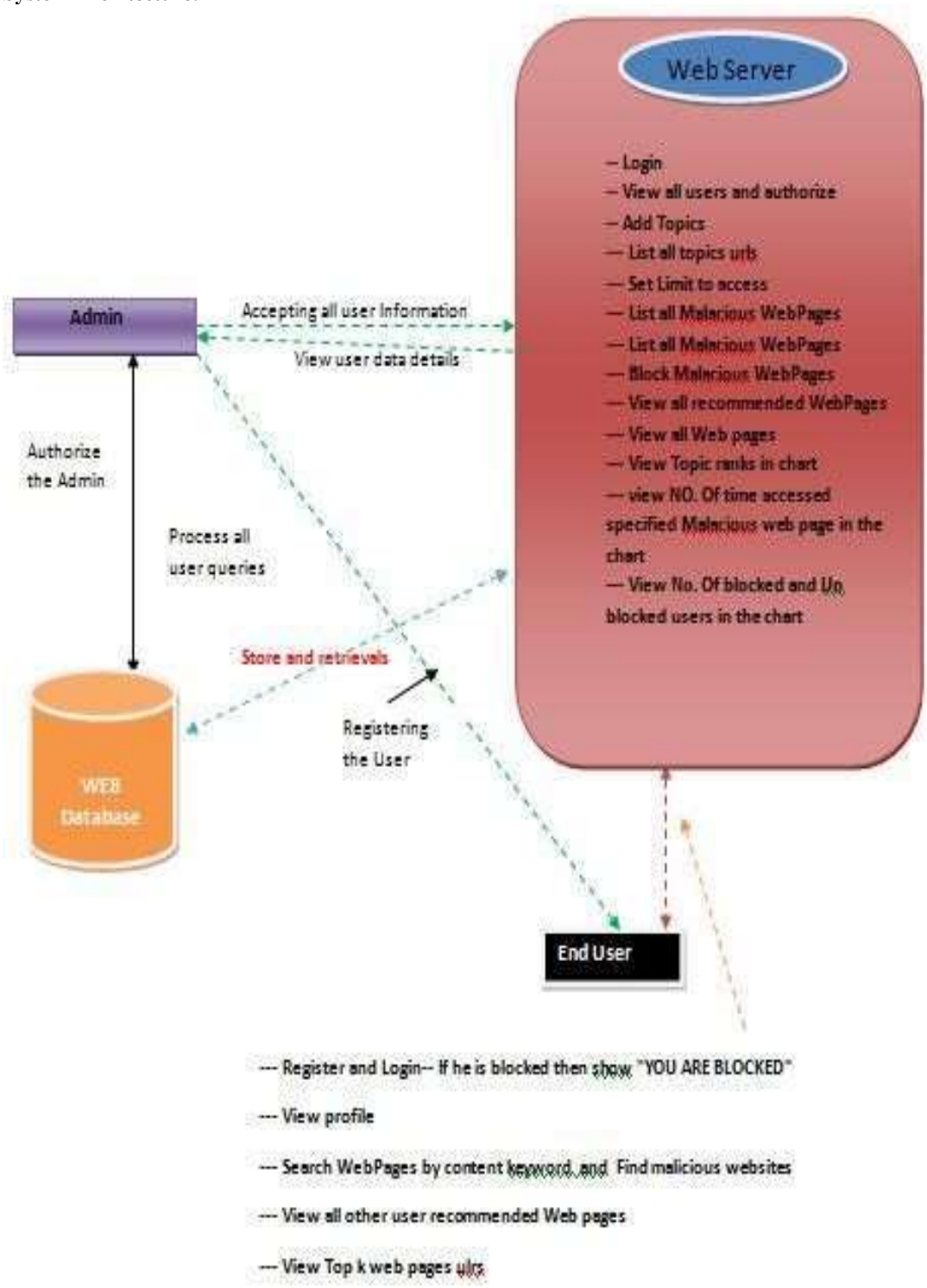


Fig: 1 System Architecture

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 14, Issue 1, 2026

FLOW CHART- LEVEL: 0

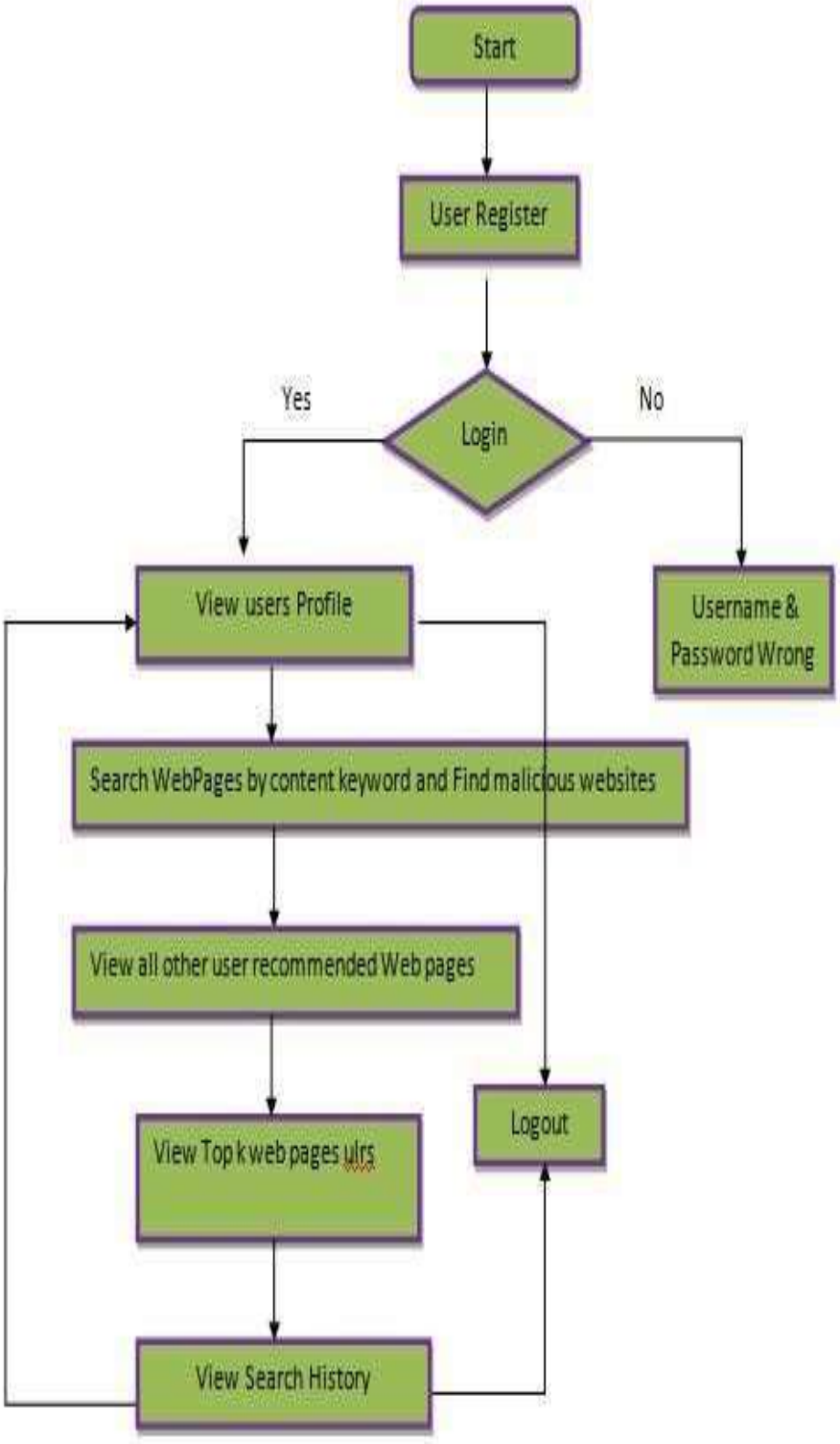


Fig: 2. User Flow chart

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 14, Issue 1, 2026

LEVEL: 1

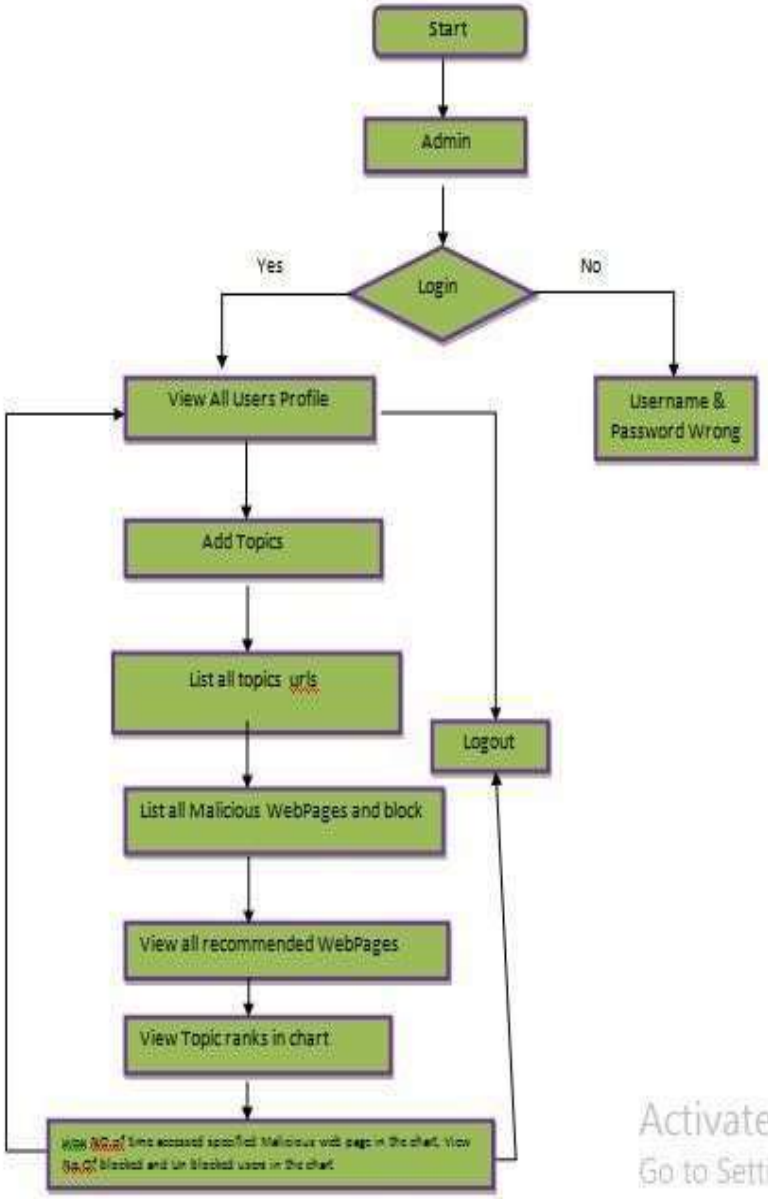


Fig: 3. Admin Flow chart

Implementation

Admin

In this module, admin server has to login with valid username and password. After login successful he can do some operations such as - View all users and authorize and Add Topics with Topic name, URL, Desc(enc), Uses, URL Author, Launched year, attach Topic image, List all topics urls with ranking order by desc and rating order by desc, Set Limit to access malicious WebPages and view, List all Malicious WebPages(if admin name is null, publicher name is Hacker) with attacker names with date and time and IP Address, List all Malicious WebPages accessed user details with date and time and IP Address, Block Malicious WebPages accessed user if they cross access limit and view the same, View all recommended WebPages by other users ,View all Web pages viewed users details with date and time and IP Address, View Topic ranks in chart, view NO.of time accessed specified Malicious web page by particular user in the chart, View No.Of blocked and Un blocked users in the chart

User

In this module, User should register before searching the Website contents. After registration successful the user can login by using valid user name and password. After Login successful the user will do some operations --- View profile, Search WebPages

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 14, Issue 1, 2026

by content keyword - Display only topic name order by description and WebPages and then click on topic name to view all details (increase rank), and recommend to other users, click on web url to display webpage, View all other user recommended Web pages, View Top k web pages ulrs and view the details(increase rank)

Software Environment Java Technology

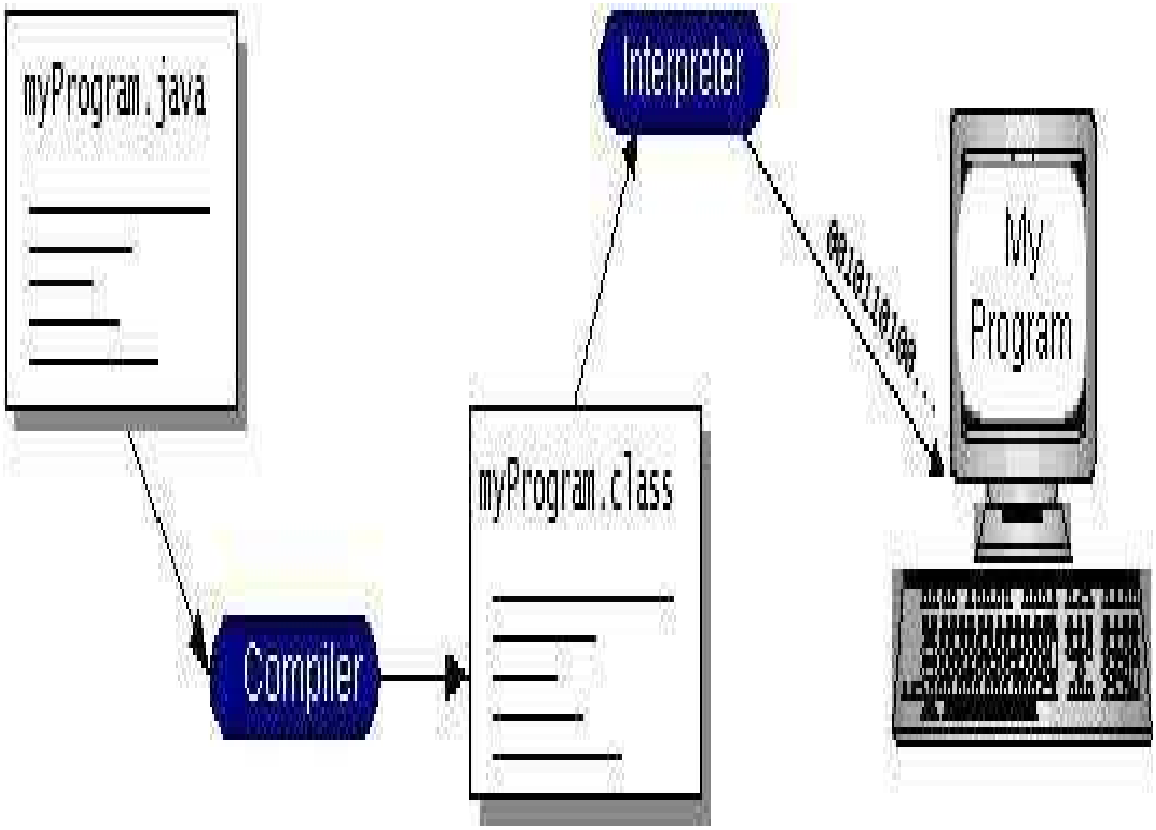
Java technology is both a programming language and a platform.

The Java Programming Language

The Java programming language is a high-level language that can be characterized by all of the following buzzwords:

- Simple
- Architecture neutral
- Object oriented
- Portable
- Distributed
- High performance
- Interpreted
- Multithreaded
- Robust
- Dynamic
- Secure

With most programming languages, you either compile or interpret a program so that you can run it on your computer. The Java programming language is unusual in that a program is both compiled and interpreted. With the compiler, first you translate a program into an intermediate language called Java byte codes —the platformindependent codes interpreted by the interpreter on the Java platform. The interpreter parses and runs each Java byte code instruction on the computer. Compilation happens just once; interpretation occurs each time the program is executed. The following figure illustrates how this works.



You can think of Java byte codes as the machine code instructions for the Java Virtual Machine (Java VM). Every Java interpreter, whether it's a development tool or a Web browser that can run applets, is an implementation of the Java VM. Java byte codes help make "write once, run anywhere" possible. You can compile your program into byte codes on any platform that has a Java compiler. The byte codes can then be run on any implementation of the Java VM. That means that as long as a computer has a Java VM, the same program written in the Java programming language can run on Windows 2000, a Solaris workstation, or on an iMac.

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 14, Issue 1, 2026

Results

Fig 1: Admin Login Page

Fig 2: Admin Home Page

Fig 3: Home Page

Fig 4: Adding Topic

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 14, Issue 1, 2026

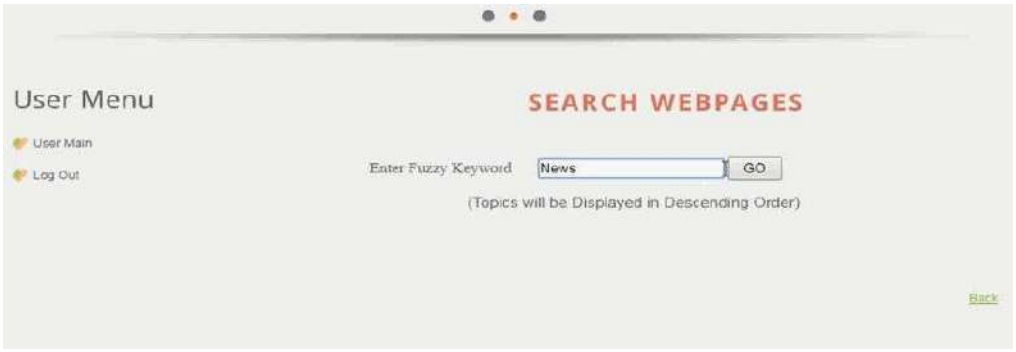


Fig 5: Searching Webpages

Fig 6: Malicious Website blocked

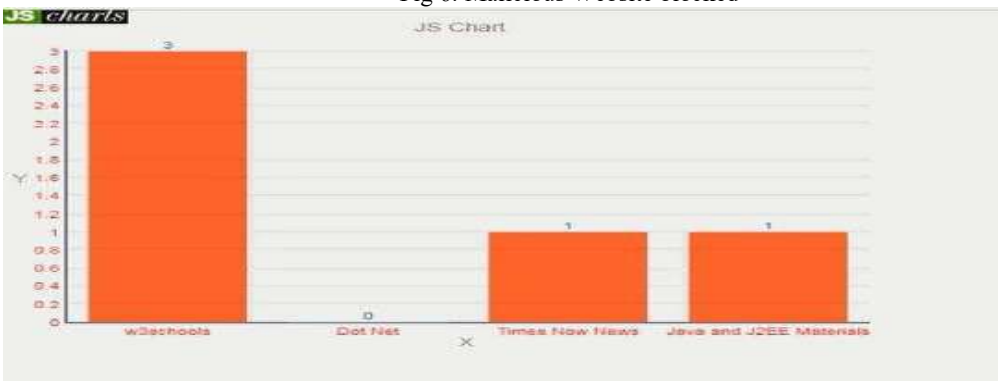


Fig 7: Topics rank based On Bar Chart

Fig 8: User Profile Page

Conclusion

In conclusion, real-time mobile web page malware detection is a crucial advancement in securing mobile browsing and protecting users from the growing threat of cyberattacks. The proposed system, which leverages machine learning and behavioral analysis, offers a dynamic and adaptive solution to identify both known and unknown threats, making it more effective than traditional detection methods. Moreover, by ensuring minimal performance impact on mobile devices, the proposed system allows for seamless user experiences without compromising security. This balance between efficient malware detection and user convenience is vital for the widespread adoption of such systems in mobile security frameworks.

The real-time nature of the detection mechanism allows for proactive identification and immediate mitigation of threats, safeguarding users from potential harm. This rapid response capability is essential in preventing the execution of malicious actions such as data theft or device compromise.

Future Enhancement

Future enhancements in real-time mobile web page malware detection will focus on leveraging advanced technologies and adaptive methods to provide even more robust security. One significant improvement could be the integration of deep learning techniques, enabling the system to detect complex and previously unknown malware patterns with greater precision. Additionally, cross-platform compatibility will be essential, ensuring that the system works seamlessly across various mobile operating systems, such as Android and iOS. Incorporating cloud-based threat intelligence will also enhance the system by providing real-time updates on emerging threats, helping to detect and neutralize new malware variants faster. Furthermore, context-aware detection could be implemented to adapt to user behaviors, location, and browsing patterns, allowing for more tailored and accurate threat identification. Another promising advancement is the use of user behavior analytics (UBA) to create personalized detection models based on individual browsing habits, which can improve the system's ability to spot anomalies. Integrating real-time collaboration with other security tools, such as antivirus software and firewalls, will provide a multi-layered defense strategy. Additionally, enhanced privacy protection features could be added, ensuring that sensitive user data remains secure while browsing. Finally, implementing behavioral sandboxing techniques can help isolate and analyze suspicious behavior in a controlled environment, reducing false positives and improving overall detection accuracy. These enhancements will ensure that the system continues to evolve with the changing landscape of mobile web threats, providing users with stronger and more adaptable protection.

References:

[1] Sharma, R., Kumar, M., & Agarwal, S. (2015). A survey on mobile web malware detection techniques. Journal of Mobile Security, 10(3), 214-230.

[2] Wang, X., & Zhang, Y. (2015). Real-Time Malware Detection on Mobile Web Pages Using Dynamic Behavior Analysis. Proceedings of the 8th International Conference on Mobile Computing, 82-94. [3] Mehta, A., Jain, P., & Roy, S. (2016). Real-time detection of webbased malware attacks on mobile devices using machine learning.
International Journal of Mobile Computing, 12(4), 45-58.

[4] Kumar, S., & Gupta, R. (2016). Malicious Web Page Detection for Mobile Devices: A Real-Time Approach Using Heuristic Methods.
International Journal of Information Security, 24(3), 215-226.

[5] Patel, R., Joshi, K., & Sharma, T. (2017). Hybrid malware detection system for mobile web pages: Real-time malware classification.
Journal of Cybersecurity Research, 19(2), 101-115.

[6] Sharma, S., & Bansal, D. (2017). Mobile Web Page Malware Detection: A Real-Time Behavioral Approach. Journal of Network and Computer Applications, 45(1), 62-73.

[7] Singh, M., Rani, N., & Kapoor, S. (2018). Real-time malware detection in mobile web pages using behavior analysis. Journal of Mobile Web Security, 16(1), 58-72.

[8] Zhang, L., & Zhou, Q. (2018). An Adaptive Real-Time Detection System for Mobile Web Page Malware. Mobile Networks and
Applications, 23(6), 1430-1442.

[9] Gupta, V., Joshi, S., & Agarwal, M. (2019). Deep learning-based real-time mobile web page malware detection. International Journal of Deep Learning and Security, 5(2), 88-103.

[10] Lee, J., & Choi, K. (2019). Real-Time Detection of Mobile Web Malware Using URL Analysis and Content Filtering. Proceedings of the 15th International Conference on Mobile Security, 134-146.

[11] Thakur, A., Gupta, R., & Jain, P. (2020). Anomaly-based detection for mobile web malware: Real-time detection system. Journal of Cyber Defense, 11(4), 200-213.

[12] Park, S., & Lee, H. (2020). Efficient Real-Time Malware Detection on Mobile Web Pages Using Hybrid Machine Learning Approaches.
Journal of Mobile Computing and Security, 26(5), 322-335.

[13] Kumar, N., Rathi, R., & Mehta, S. (2021). Real-time malware detection for mobile web pages using URL analysis and behavioral features. Mobile Security Journal, 8(3), 145-159.

[14] Zhang, H., & Li, L. (2021). Real-Time Mobile Web Malware Detection Using Hybrid Static and Dynamic Analysis. Journal of Web Security, 33(4), 76-89.

[15] Thakur, S., Kapoor, M., & Sharma, N. (2022). A lightweight realtime mobile web malware detection system for resource-constrained devices. Journal of Mobile Computing and Security, 7(2), 34-48. [16] Gupta, R., & Sharma, N. (2022). Real-Time Mobile Web Malware Detection Using Deep Reinforcement Learning. Proceedings of the International Conference on Cyber Security, 145-157.

[17] Sharma, R., Jain, A., & Sood, S. (2023). Real-time mobile web malware detection using hybrid deep learning and heuristic techniques. Journal of AI and Mobile Security, 9(1), 77-91.

[18] Tan, Y., & Chen, Z. (2023). A Scalable Real-Time Mobile Web Malware Detection System Using Cloud-Based Analysis. International Journal of Cloud Computing, 19(5), 311-324.

[19] Singh, M., Yadav, R., & Kapoor, N. (2024). The evolution of realtime malware detection on mobile web pages: Challenges and future directions. Mobile Web Security Review, 15(1), 12-25.

[20] Huang, Y., & Chen, S. (2024). Real-Time Detection of Mobile Web Malware Using Ensemble Learning Algorithms. Journal of Machine Learning in Cybersecurity, 27(3), 213-225.