Ad Block and Malicious URL Detection System

Aditya V Shetty
Dept. of Computer Science and Engineering
Alva's Institute of Engineering & Technology
Mangalore, India

Algeena Carol Dsouza
Dept. of Computer Science and Engineering
Alva's Institute of Engineering & Technology
Mangalore, India

Aditya Maruti Naik
Dept. of Computer Science and Engineering
Alva's Institute of Engineering & Technology
Mangalore, India

Reena Lobo
Prof. Dept. of Computer Science and Engineering
Alva's Institute of Engineering & Technology
Mangalore, India

***Abstract*—The main aim of this project is to provide an easy and smooth browsing experience over the internet. This is to mainly optimize the user experience of surfing through various web-pages. Users mainly get frustrated due to redirecting of page to annoying web-pages. To add to this, suppose the wi-fi , Ethernet or relative service's network is weak, this redirection causes a tedious task for the user to search or obtain the required result. Our project focuses on these drawbacks and will try to improve the user's browsing experience by blocking unwanted notification popups and redirection of website automatically. It also allows user to access the website only after user's approval to visit that website. It also keeps track of recently visited website with the help of cookies. This project helps user to protect their device by stopping them from entering malicious websites and also get rid of multiple popups**

Keywords—Malicious websites, popups, redirection, unwanted notification and multiple popups, protection, security and secure.

I. INTRODUCTION

Users are completely dependent on internet as the rapid growth in generation this generation is also known as internet era. People all around world use internet. The growth in percentage of internet usage all around the world is around 1,052% during 2000-2018 according to Internet Usage Statistics. Users are fooled many times by stealing their useful information. Many users will do online transactions and store their useful information like username and password for easy usage during next transaction or login. Sometimes during the transaction, clicking on ads browsing redirection of website takes place and user might end up in some harmful website or multiple popup might flash on screen with multiple tab opening, which might contain harmful malware or viruses. It may help hacker to steal user credentials during browsing. Main aim of the project is to overcome this problem faced by users all over the world.

Out of the many problems faced by internet users today, few are unwanted redirection, and repeated annoying ads. One's user experience can be spoiled if the user accidentally visits some malicious website, which may be a host for Google redirect viruses for the user. Any form of the Google Redirect Virus is dangerous due to the malicious commands it executes and the stealth programming techniques used to hide its files from prying eyes and anti-virus software radars. This project's main goal is to focus on improving user experience using internet.

There are various systems available in the market today which promises to provide facility of blocking ads, which has been not very accurate in performing task. This project mainly focuses on:

- Verifying re-direction of webpages by the user.
- Blocking annoying ads.
- Alerting the user before entering an unsecured site.

This project's implementation will seek user's permission before redirecting the user from current page to some other page by popping up URL, be this redirection genuine (i.e. 301 redirection or 302 redirection) or some malicious redirection. Manual cache clearing will reduce the distraction of user from repeated ads. Blocking ads will surely improve user experience using the internet.

II. LITERATURE SURVEY

A. Related Work

Ashish Kumar Singh et.al [1] explains how ads can be blocked in any websites and why should we block some unwanted ads. It also mention how useful it will be if ad is blocked and it will increase user browsing experience. Jing Wang et.al [2] presents paper on Systematic Discovery of Unvalidated Redirects and Forwards in Web Application which helps in understanding how http websites can leak personal information of users and disadvantages of http websites and ads.

Zhou Li et.al [3] presented a paper on Understanding and Detection of Mass Redirect-Script Injections which describes approach analyzes the difference between a suspicious JS-lib file and its clean counterpart to identify malicious redirect scripts. Kurt Thomas et.al [4] presented a paper on Design and Evaluation of a Real-Time URL Spam Filtering Service that explains about the spam URL detection, which helps user to study about spam URL.

OmidAlipourfard et.al [5] presents paper on A Comparison of Performance and Accuracy of Measurement Algorithms in Software which describes the accuracy of software after the successful development. Measurement of critical ad blocking system, which helps user to increase browsing experience. Elliott L. Post et.al [6] presents a paper on Comparative Study and Evaluation of Online Ad-blockers which describes how ad block system requirement changes and it fails to block the ads. It also describes how system fails to detect new ads in website. Elias Konidis et.al [7] presents the paper on Evaluating Traffic Reduction Mechanisms for High Availability Servers which explains about the availability of cloud applications and their respective server high availability.

Detecting Malicious Website by Integrating Malicious, Benign, and Compromised Redirection paper is presented by Toshiki Shibahara et.al [8] it helps user to understand how software are compromised in redirection and how it is harmful. Anant Agarwal et.al [9] presented paper on reducing the miss rate of direct mapped caches it reports how direct mapped caches are popular design choice for high performance. Sangho Lee et.al [10] presented paper on Detecting Suspicious URLs in Twitter Stream. Which helps us to understand how Twitter and other social media detect and stop harmful URLs.

B. Gaps in Exisiting System

- Currently there is no application that stops redirection of the website and prevents multiple tab opening which might be one off the harmful website.
- Advertisements blocking application currently being used promotes their own ads to gain profit and post ads. Which does not makes user complete ad free.
- All the application which exists are ad block system but it does not have manual cache clearing option to the user, which helps to remove ads present inside cache for long time.
- Users are less not satisfied with the current ad block system which is freeware but promotes their own ads by different ways, and also fools people by wasting their internet in backend and download their own promoted application.

C. Problem Satetment

As internet users are rapidly increasing nowadays, to gain profit through internet third party software get into user and post ads and transfer user information and this leads to security problem. User browsing experience is decreasing ever day by allowing some third party software into their browser or system. User will not be having any idea about the harmful website they visit.

III. IMPLEMENTATION

A robust ad block and malicious URL detection system is developed. Browser level extension is developed to safeguard user personal information. JavaScript, Jason and java language is used to implement extension to any browser like chrome, Internet Explorer, Chrome, Firefox.

A. JavaScript and Jason for pattern match

JavaScript and Jason are robust and powerful language used to develop extension. Pattern match technique is used to recognize ad patterns in any websites, if ad pattern matches in background with website then it identifies it as ads and block the particular. Set of Jason code helps in searching malicious URL set in background and make sure user is not visiting malicious or phishing noted URLs in background. It enables security features as it is not easy to break into system. Jason language is easy in implementation which reduces complexity of coding in extension.

B. Malicious URL detection and avoidance

Extension is developed in such a way that it contains set of malicious URL in backend, whenever user knowingly or unknowingly visit any malicious sites through ads, popups or unwanted redirection, Extension make sure the entered website is secure website and it is not present in malicious URL list.

If user enters any malicious URL, tree stops and redirection is stopped. This solves security issues of daily life. Phishing list is updated in background and can also be imported or manually added by any user using extension.

Redirection of any website automatically stopped and it is validated first made sure that it is secure connection established between user and server. Many websites transfer virus through ads or by clicking on some link, user will be directed to some random unsecure website to steal user personal information. This extension helps to provide high security to all user and increases browsing experience without any ads.

C. Algorithm or pseudo code for extension

Algorithm helps to understand working of extension in simple words. It is step by step implemention and working of extension.

Step1: Start
Step2: Install extension.
Step4: Accept URL.
Step5: Validate URL.
- Compare with blacklisted URL.

Step6: If validate
- Create TCP connection.
- Download data.
- Scan page script.
- Block ads if present.

Step7: Else
- Close Tab.

Step8: End

User initially need to install extension into any of the browser. When user enters any of the URL, extension validates the URL entered by user and if it is secure URL then it redirects to particular website otherwise it will be found in blacklisted website and it stops redirection to that website.

Pattern match technique is used to recognize ad pattern and ads are blocked. Page scripts are compared with genuine websites and malicious URL and ads are blocked. Unwanted redirection is stopped for security breakage to make sure user only visit secure websites. Whenever by mistake user clicks on any unsecure link it gets redirected, to stop this security breach in present system this extension is used. This reduces

the number of phishing attacks, user information is secured and increases browsing experience of the user. This is working of algorithm which enables high security while browsing in internet. It also warns http websites are not secure. This helps layman using browser and secure user data and warns user whenever they visit any malicious websites.

D. Architecture Diagram

When user uses any browser AdBlockSystem gets activated and when user enters URL it checks validation of UTL and warns if it is not secure URL. If URL is noted malicious then user get warning message saying its malicious website do not enter and it also block ads to increase browsing experience and secure surfing.

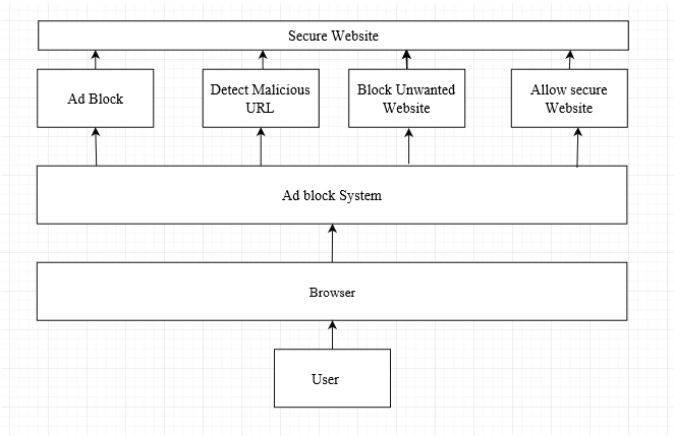

Fig. 1. Architectural Block Diagram

IV. CONCLUSION

The proposed system is successfully run on Google chrome browser on a machine running Windows 10 platform. The proposed system is successfully blocking the blacklisted sites with a performance rate of 100 percent, and is also showing acceptable results in case of blocking ads and completely efficient in alerting users when the website, user trying to visit is not secure.

V. FUTURE WORK

The add blocking part of the proposed system can be enhanced further.

REFERENCES

[1] Ashish Kumar Singh and Vidyasagar Potdar, Blocking Online Advertising –A State of the Art, Digital Ecosystems and Business Intelligence (DEBI).Institute, IEEE, 2009.

[2] Jing wang and Hongjunwn, URFDS: Systematic Discovery of Unvalidated Redirects and forwards in Web Applications: Jing Wang School of Physical and Mathematical Sciences, Nanyang Technological University IEEE, CNS, 2015.

[3] Zhou Li, Sumayah Alrwais, XiaoFeng Wang, Eihal Alowaisheq, Hunting the Res Fox Online: Understanding and Detection of Mass Redirect-Script Injections, Indiana University at Bloomington: RSA, Laboratories, IEEE, 2014.

[4] Kurt Thomas, Chris Grier, Justin Ma, Vrn Paxson, Dawn Song, Design and Evaluation of a Real-Time URL spam Filtering Service, University of California, Berkeley International Computer Science Institute, IEEE, 2011.

[5] R. Omid Ali pourfard Masoud Moshref, Yang Zhou and Minlan Yu A Comparsion of performance and Accuracy of Measurement Alogorithms in software:March,2018.

[6] Elliott L. Post and Chandra N Sekharan, Comparative Study and Evaluation of Online Ad-blocker Department of Computer Science, Loyola University Chicago, IEEE, 2015.

[7] Elias Konidis, Panagiotis Kokkinos and Emmanouel Varvarigos Dept of Engineering and Informatics@ceid.upatras.gr ,IEEE, 2017.

[8] Toshikishibahara yutatakata mitsuakiakiyama, takeshiyagi, takeshiyadaDEtecting malicious websites by intergation malicious, benig, and compromised redirection subgraph similarities ntt secure platform laboratories, Tokyo, Japan.IEEE, 2016.

[9] Anant Agarwal and Steven D.pudar, A Technique for Reducing the Miss Rate of Direct-Mapped Caches, Laboratory for Computers Science , Massachusetts Institute of Technology, Cambridge, MA02139.IEEE,1993.

[10] Sangho Lee and Jong Kim, Detecting Suspecious URLs in Twitter Stream, Department of Computer Science and Engineering Divison of IT Convergence Engineering, Pohang of Korea,IEEE,201