Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 3, March 2015, pg.339 – 344

RESEARCH ARTICLE

WEB REPUTATION BASED ON INTELLIGENT DECISION ENGINE WITH RATINGS AND CATEGORY

T.Mugilan
Assistant Professor
Department of Computer Science and Engineering
IFET College of Engineering, Villupuram, Tamil Nadu
mugipdy@gmail.com

D.Thenmozhi
BE Student
Department of Computer Science and Engineering
IFET College of Engineering, Villupuram, Tamil Nadu
honyla93@gmail.com

Abstract: Web reputation is the methodology used to determine whether the website is malicious is not. To determine the reputed websites many methods are available such as user ratings, Qos service, single anti-virus engine and multiple anti-virus engines. We introduce a new modus operandi irate Intelligent Decision Engine. It is a URL or Domain scanner which gives rating on website (Bad or Safe to visit) for a given domain. Basically it works like a MAV engine (Multiple Anti-Virus), but here it gets the ratings from various top security domains that provide the rating of the given domain. Added to this it checks whether the domain or URL gives is present in any of the domain blacklist sites and provides iCategory. The proposed system gives an analyst an advantage of having the Domain rating for the given domain with a lookup on top blacklist providing sites and also the Category Classification for the given domain.

Keywords: Web reputation, Anti-malware engine, scan, safe

I. INTRODUCTION

Web service technology creates an atmosphere where users and applications can search and compose services in a habitual and flawless manner. In the service-oriented atmosphere where everybody is allowed to propose services, it is natural that there will be plentiful offers of services providing comparable or similar functionality. However, some Web services may perform maliciously. It is not an easy task since some service providers may not fulfill their promised service quality. The reputation of Web service needs to be considered when making a service selection. Web service reputation is regarded as a metric of its future behavior. It is a collective measurement of the opinions of a community of users regarding their actual experience with the Web service. Web Reputation is the newest and

finest method to enhance the protection against contemporary to prospect malicious content on the web for those browsing the Internet. Using Web Reputation, websites are assessed for instant and prospective threats, malicious content and perilous characteristics. In an analogous way that Content Categorization places websites into different categories and classify them based on their content, Web Reputation score is used to determine the risk factor of each website. Once the score for a website has been determined, this will help an proprietor to take action – block/proceed with caution/allow access to those websites. Although a good antivirus engine offers significant threat coverage, and multiple antivirus engines provide greater protection than you get with a single antivirus engine, it is very obscure to achieve total security in a very dynamic Web 2.0 world. Web Reputation fills an invalid left by habitual protection engines by giving a "safety" rating to websites and where necessary, allowing positive blocking of precarious sites.

II. BACKGROUND AND RELATED WORKS

A. Reputation Measurement and Malicious Feedback Rating Prevention in Web Service Recommendation Systems:

This existing system preclusion scheme contains two stages, i.e., activating stage and blocking stage. A malicious feedback ranking over a Web service can be blocked with high prospect by querying whether its IP is a member of S, assuming that the RSB could proficiently run. Hence, the anticipated prevention scheme can block malicious censure ratings with high success probability. Moreover, it can support diverse development environments of reputation systems with special phony positive probability constraints. The Bloom filter guarantees no false negative, and in an supreme case, the success prospect could reach 100%. But the proposed prevention scheme cannot wedge malicious feedback rating with 100% prospect because of these existing factors such as active IP addresses, the low power of malicious feedback ratings and so on. Hence, the legalization demonstrated that our projected prevention scheme can block the malicious feedback ratings with very elevated probability.

B. Evaluating Feedback Ratings For Measuring Reputation Of Web Services:

In the field of examine computing, reputation of a Web service is usually calculated using response ratings provided by examination users. However, the existing of malicious ratings and different preferences of different service users regularly lead to a prejudice towards positive or pessimistic ratings. A narrative reputation measure method for Web services is proposed. The proposed method employs two phases (i.e., malicious rating exposure and rating adjustment) to develop the reputation measure accuracy. Firstly malicious feedback ratings by the Cumulative Sum technique are detected, and then diminish the affect of dissimilar user feedback preferences by using Pearson connection Coefficient. Extensive experiments are conducted. Experimental outcome show that our planned method is efficient and can enhance the consistency of service selection.

C. A Scalable Hybrid Collaborative Filtering Algorithm for Personalized Web Service Recommendation

Numerous approaches to web service collection and suggestion via shared filtering have been studied, but not often have these studies painstaking the difference between web service commendation and product recommendation used in e-commerce sites. An original hybrid shared filtering algorithm that is designed for hefty scale web service recommendation. Diverse from other approaches, this method employs the uniqueness of QoS by edifice an efficient province model. Based on this model, web assessment recommendations will be generated swiftly by using adapted memory-based collaborative filtering algorithm. Investigational results exhibit that apart from being decidedly scalable, Region KNN provides extensive enhancement on the recommendation exactitude by comparing with other well-known collaborative filtering algorithms.

D. Collaborative Reliability Prediction Of Service-Oriented Systems

Service-oriented architecture (SOA) is becoming a most important software scaffold for building composite dispersed systems. Consistency of the service-oriented systems heavily depends on the distant Web services as well as the unpredictable Internet. Designing effective and accurate reliability prediction approaches for the service-oriented systems has become an important research issue. A shared consistency prophecy approach, which employs the precedent failure statistics of other similar users to envisage the Web service consistency for the modern user, devoid of requiring real-world Web service invocations, is proposed. A user-collaborative malfunction data allocation method and a dependability symphony sculpt for the service-oriented systems. extensive real-world experiments are conducted and the tentative results illustrate that our mutual reliability prophecy approach obtains better steadfastness prediction accuracy than other approaches.

III. WEB REPUTATION USING ANTI-MALWARE ENGINES

To prevent advanced threats that might be missed by anti-malware engines from entering your organization, it can sanitize- potentially dangerous file types to thwart zero-day and targeted attacks. In addition, to identify and block files that have spoofed file type extensions, which indicates prospective malicious intent.

The combination of scanning data with anti-malware engines first, leveraging the supremacy of their individual heuristic analyses, followed by converting potentially precarious files to remove entrenched threats greatly decreases the chances of your network being infected by an unknown threat. To provide the end user a better clarity in results provides 4 Scan engines which include top URL blacklist providers and for clear picture on URL classification, it has 3 major category classification sites.

- AVG Threat Labs
- Norton Safe Web–Symantec
- Site Advisor-McAfee
- Web Security Guard
- Multiple engines are scan one by one it's not affect the system like freezes
- The virus definitions are reorganized automatically.
- It scans each and every domain is present in that link.

IV. SYSTEM ARCHITECTURE

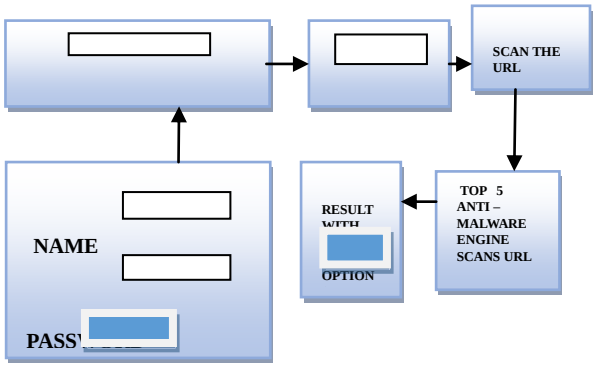

Figure 1: System Architecture

In this section we present the overall process of the web reputation using anti-malware engine.

Figure 1 illustrates the architecture of our system. This system architecture consists of four modules.

It includes endorsement, search, scan, and upshot.

A. ENDORSEMENT

In this module user creates their username and register. After that user can enter in to the irate decision engine using that username. New user can make a registration and perform the task. Administrator has authority to wedge and Accept the website and review the details of the entire website .Administrator have authority to allow the registered user to search. The process of identifying an individual usually based on a username and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual. Authentication is the initial step for all process. Because authentication is confidentiality step. Only registered user can proceed the next step.

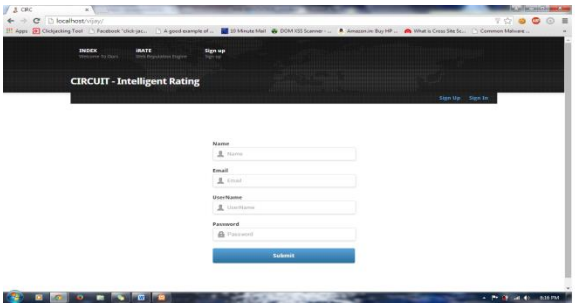

Figure 2: Signup form

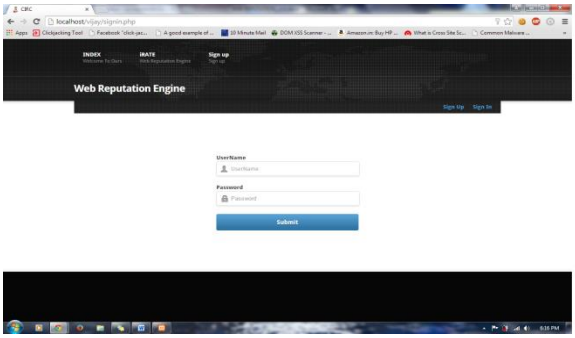

Figure 3: SignIn Form

B. SEARCH

In this module user gives the domain name or an URL which will be scanned by the Anti-Malware engine. It will search the URL which is given by user in the blacklist and WHOIS list. From that it is very easy to know about the domain. Each and every websites in the internet are registered in the WHOIS list. **WHOIS** is an inquiry and response protocol that is broadly used for querying databases that hoard the registered users or assignees of an Internet resource, such as a field name, an IP address block, or an independent system, but is also used for a broader range of other information. The protocol supplies and delivers database content in a human-

readable format. If the given domain not in the WHOIS list, it will be considered as a fake domain. Then it will not be scanned by the Anti-Malware engines. It also checks blacklist whether the given domain is already blocked or not.

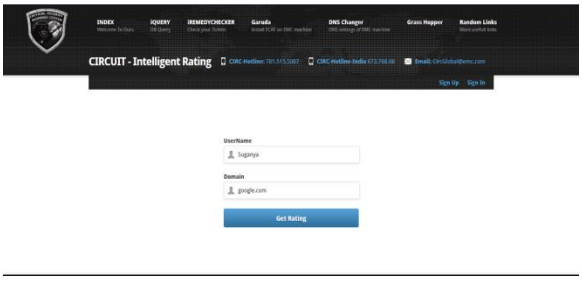

Figure 3:Search the URL in the blacklist

C. SCAN

In this module given URL will be scanned by the anti-malware engines such as AVG Threat Labs, Norton Safe Web–Symantec, Site Advisor-McAfee, Web Security Guard, URLvoid. These anti-malware engines are top anti-malware engine. It will provide the accurate result about the domain. Because these malware engines update automatically. No need to spend time. Scans the given URL according to Anti-malware engines in Explore module, are to be called, in which URL has filtered and, finds the vulnerable links if available in those pages.

Advantage is able to scan five different malware engines together, so we can catch the vulnerable links easily. Some URL cannot be tested.URL is scanned by anti-malware engine simultaneously. Trend URL and McAfee site advisor provide the URL category.

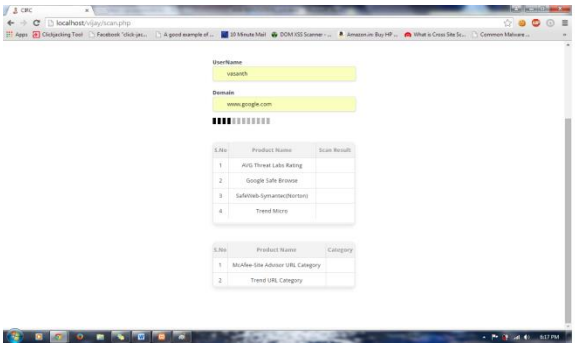

Figure 4: Scanning the URL

D. UPSHOT

In this module scan result is displayed. After scanning the given domain scan result is represented by the color such as green, red and gray. Green color represents the given domain is safe. Red color represents the given domain is vulnerable. Gray color represents the given domain is untested (i.e. some domains cannot be scanned).Anti-malware engine also provide the category of the given domain. New viruses also detected by the anti-malware engine. Because anti-malware engines are updated automatically. New features of anti-malware engines can be easily updated due to internet connection.

If suppose given domain is detected as vulnerable then that domain can be blocked in our own system.

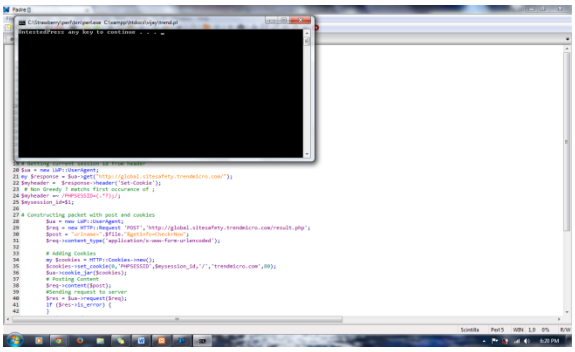

Figure 5:Scan Result

V. CONCLUSION

This paper proposed a new technique to determine the reputed web sites. Top 5 anti-malware engines are used to scan the domain. The output will be very efficient than other methods. End user get a better clarity in results provides 4 Scan engines which include top URL blacklist providers and for clear picture on URL classification, Future implementation cloud Antivirus for each and every one that can be secure and which has huge database for scanning the website ,that also can be implementable for file scanning also.

REFERENCES:

1. S. Wang, Z. Zheng, Q. Sun, H. Zou, and F. Yang. "Evaluating feedback ratings for measuring reputation of web services". In Proceedings of the IEEE International Conference on Services Computing (SCC'11), pages 192-199, 2011.
2. X.Chen, X. Liu, Z. Huang, and H. Sun. RegionKNN: "A scalable hybrid collaborative filtering algorithm for personalized web service recommendation", In Proceedings of the 8th IEEE International Conference on Web Services (ICWS'10), pages 9-16, 2010.
3. Z.Zheng and M. R. Lyu. "Collaborative reliability prediction of service-oriented systems". In Proceedings of the 32nd ACM/IEEE International Conference on Software Engineering (ICSE'10), pages 35-44, 2010.
4. N.Limam and R. Boutaba. "Assessing Software Service Quality and Trustworthiness at Selection Time". IEEE Transactions on Software Engineering, 36(4): 559-574, 2010.
5. W.Conner, A. Iyengar, T. Mikalsen, I. Rouvellou, and K.Nahrstedt. "A trust management framework for service-oriented environments". In Proceedings of the 18th international conference on World Wide Web (WWW'09), pages 891-900, 2009.
6. S.Nepal, Z. Malik, and A. Bouguettaya. "Reputation Propagation in Composite Services". In Proceedings of the IEEE International Conference on Web Services (ICWS'09), pages 295-302, 2009.
7. D.Ardagna and B. Pernici. "Adaptive service composition in flexible processes". IEEE Transactions on Software Engineering, 33(6): 369-384, 2007.
8. R.Jurca, B.Faltings, and W. Binder. "Reliable QoS monitoring based on client feedback". In Proceedings of the 16th international conference on World Wide Web (WWW'07), pages 1003-1012, 2007.
9. Z.Malik and A.Bouguettaya. "Evaluating rater credibility for reputation assessment of web services". In Proceedings of the 8th International Conference on Web Information Systems Engineering(WISE'07), pages 38-49, 2007.
10. Z.Xu, P. Martin, W. Powley, and F. Zulkernine. "Reputation enhanced QoS-based web services discovery". In Proceedings of the IEEE International Conference on Web Services (ICWS'07),pages 249-256, 2007.

