WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Integrated Fuzzy based Computational Mechanism for the Selection of Effective Malicious Traffic Detection Approach

J.Lekanjani [#1]***, M.Hemamalini*** [#2]

[#1] M.Sc, Department Of Computer Science, Kamban College Of Arts And Science For Women, Tiruvannamalai-606603

[#2] Assistant Professor, Department Of Computer Science, Kamban College Of Arts And Science For Women, Tiruvannamalai-606603

ABSTRACT

A mechanism to effectively detect malicious traffic in the present context where new cyber criminals and threatening actors are emerging every day, has become a compelling need. These invaders use overwhelming tactics that mask the nature of attacks and make bad acts seem innocuous. A growing number of trustworthy electronic systems and facilities have been introduced with the fast development of pervasive digital technologies. However threats to cyber-security continue to grow, posing hindrance in the efficient use of digital services. The detection and classification of malicious traffic due to security threats can be done by an efficacious traffic detection approach. The development of a smart, precise malicious traffic detection system has therefore become a subject of extensive research. Current traffic detection systems are typically employed in conventional network traffic detection. These systems sometimes face failure and cannot recognize many known or modern security threats. This is because they rely on conventional algorithms which focus less on precise selection and classification of functions. . To keep up productivity of web security, these malignant URLs must be recognized, distinguished just as their comparing connections ought to be discovered. Subsequently clients get shielded from it and viability of system security gets expanded. For such ID there must be analyser which ought identify such URLs as well as. What's more, strategies to recognize relating connections of noxious URLs .This methodology will keep the clients from assaults and increment effectiveness of web creeping stage.

KEYWORDS: MAlicious url, Ranking clustering

1.introduction

Nowadays, the world is witnessing a proliferation of the web with various inventions and technical advances. Innovations in industry have compelled the companies and authorities worldwide to develop and use advanced networks. These networks are an integration of a number of security factors including encryption, data completeness, authentication, and innovations such as distributed database systems, Internet voice, wireless connectivity, and web servicesThe World Wide Web and new communications technologies drive new opportunities for commerce; they inevitably create new opportunities for criminal actors as well. Today millions of rogue Web sites advance a wide variety of scams including marketing counterfeit goods, perpetrating

financial fraud (e.g., “phishing”) and propagating malware (e.g., via “drive-by” exploits or social engineering). What all of these activities have in common is the use of the Uniform Resource Locator (URL) as a vector to bring Internet users into their influence. As a result, it is a challenging task to identify malicious pages as they appear on the web. However, it is critical to succeed at this task in order to protect web users.

The technology in current virus scanner has two parts: a signature-based detector and a heuristic classifier that detects new viruses. This kind of analysis can be time consuming and oftentimes still fail to detect new malicious executable. Searching for malicious web pages is a three-step process, in which URLs are first collected, then examined in depth using specialized analysers for classifying web pages or URLs as malicious and benign then last step is submitting these malicious URLs to different methods to search their corresponding links said to be as initial seed. To collect URLs, one typically uses web crawlers, which are programs traversing the web in a systematic fashion. Starting from a set of initial pages, this program follows hyperlinks to find as many (different) pages as possible. To address Web-based attacks, a great effort has been directed towards detection of malicious URLs. A common countermeasure is to use a blacklist of malicious URLs, which can be constructed from various sources, particularly human feedbacks that are highly accurate yet time-consuming. The malware

analysis techniques help the analysts to understand the risks and intensions associated with a malicious code sample. Analytical method used in this paper, a classification model based on features which **built with through machine learning.**

Literature survey:

[1] **C. Leckie**In this paper, we introduce a practical scheme to defend against distributed denial of service (DDoS) attacks based on IP source address filtering. The edge router keeps a history of all the legitimate IP addresses which have previously appeared in the network. When the edge router is overloaded, this history is used to decide whether to admit an incoming Ip packet. Unlike other proposals to defend against DDoS attacks, our scheme works well during highly-distributed DDoS attacks, i.e., from a large number of sources. We present several heuristic methods to make the IP address database accurate and robust, and we present experimental results that demonstrate the effectiveness of our scheme in defending against highly-distributed DDoS attacks

[2] **Rajeev Kumar**,Security is a peak significant quality element in the pitch of software engineering. Software security improvement is easily done with the support of factors, models and metrics of security. Software security should be analyzed with the help of its security factors. Security dimension is the main attribute in evaluation, executing, and calculating security in the way to organize and develop quality of software. It is to be identified that qualifications of security factors increased through inspecting damages, discriminating susceptibility and attacks in design development process. This review is discussing the description and categorization of accessible security properties. Durability is an attribute of security that refers to the capability of software to conclude of a creation on time. Software security is affected with security attributes as well as durability. A stable state of the secure software enhances additional security

[3]**Ansari, M. T. J., & Pandey, D**Numerous malicious attempts on Networks, like DDoS, and ORM, are among the most critical issues in today's society. DDoS is a significant source of data. DDoS cyber-attacks are becoming a common worldwide internet disruption. Since these assaults/threats require network services and transport levels where verification of whether the access is legitimate or destructive is a challenging task, it becomes difficult to protect the systems against such attacks. An association of the DDoS can conveniently misrepresent its default gateway, which hides the actual cause of the incident. DDoS attacks have two targets. The first target is to use the host's resources and the second is to use the network's throughput. The present schemes for safeguarding the host's resources include drop input packets by fields. These schemes could be the protocol type or the port number.

[4] **Sahu, K., & Srivastava, R. K** Preventive checks aim to prevent undesirable incidents, while detective checks aim to recognize unwanted incidents after they arise. Usually, the IDS is utilized as a detective search to alert people about abuse and to provide details about the frequency of the incident. Such detective controls incorporate signature-based approaches as well as uncommon traffic analysis and antivirus scanners. This enables broader identification, but suffers from issues of false alarms. The IDS can also be employed as a preventive mechanism; the current IDS can disrupt a host's device call or disrupt the operation of the network. In this situation, the IDS needs to be changed so as to allow for this kind of operation only when the inappropriate behavior is clearly defined. In the present study, I have used different criteria for evaluating the performance of these malicious traffic detection systems at the implementation phase

[5]**M. T. J., AL-ZAHRANI, F. A., PANDEY**, DToday's healthcare organizations want to implement secure and quality healthcare software as cyber-security is a significant risk factor for healthcare data. Considering security requirements during trustworthy healthcare software development process is an essential part of the quality software development. There are several Security Requirements Engineering (SRE) methodologies, framework, process, standards available today. Unfortunately, there is still a necessity to improve these security requirements engineering approaches. Determining the most suitable security requirements engineering method for trustworthy healthcare software development is a challenging process. This study is aimed to present security experts' perspective on the relative importance of the criteria for selecting effective SRE method by utilizing the multi-criteria decision making methods.

2. PROPOSED SYSTEM

This approach is going to be used for detecting and analyzing URLs on web efficiently for classifying into malicious or not. In proposed work, analyzer classifies web pages into malicious and benign. This also classifies new malicious content added into web pages.

To find out other corresponding pages different types of methods has been added for better classification. These collected pages or URLs will be stored in dataset by proxy server. This will avoid direct contact with search engine.

Proxy server will act as firewall between user and malicious contents. The following figure indicates proposed system architecture.

3. METHODOLOGY

LINKS METHOD:-

A given input link as any suspicious URL analysed by the links method consists of all the URLs of known suspicious link. This method has the linking structure rather than directly building the web graph by having access to the raw crawling data of the search engine

CONTENT DORKS Method:-

Content dorks method searches the suspicious URLs by using known malicious keywords. These malicious keywords are taken from Google Hacking Database. All content dorks are submitted as queries to the search engine (Google). Then retrieved the URLs (links) from the results and later will submit them to the analysers.

SEARCH ENGIENE OPTIMIZATION Method:-

The objective of search engine optimization (SEO) method is to identify a cloaking technique as well as links which show benign page and its corresponding cloaked page which is set up by attackers. This Cloaking is a search engine optimization (SEO) technique in which the content presented to the search engine spider is different from that presented to the user's browser. This is done by delivering content based on the IP addresses or the User-Agent HTTP header of the user requesting the page.

DOMAIN REGISTRATION Method:-

This method identifies suspicious sequences of domain registrations. These domains are then used to create URLs that are scheduled for analysis. The URL creation consists of taking the closest known malicious registration and replacing the domain with the suspicious domain that we have just flagged.

Filter Requests:

Proxy servers can also be used to filter requests. For example, a company might use a proxy server to prevent its employees from accessing a specific set of Web sites.

The proxy server evaluates the request means the proxy provides the resource by connecting to the relevant server and requesting the service on behalf of the client

Check it in to the dataset as well as submit to the analyzer to classify the URLs as malicious and benign

BLOCK DIAGRAM:

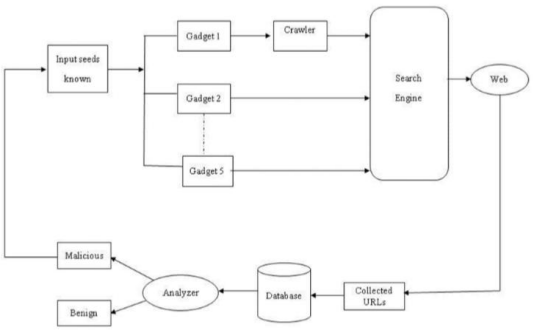
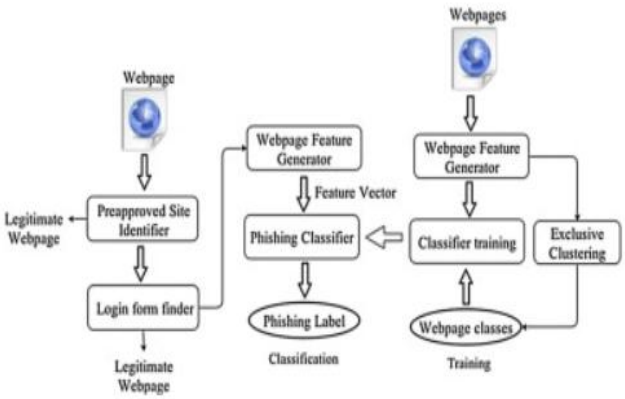
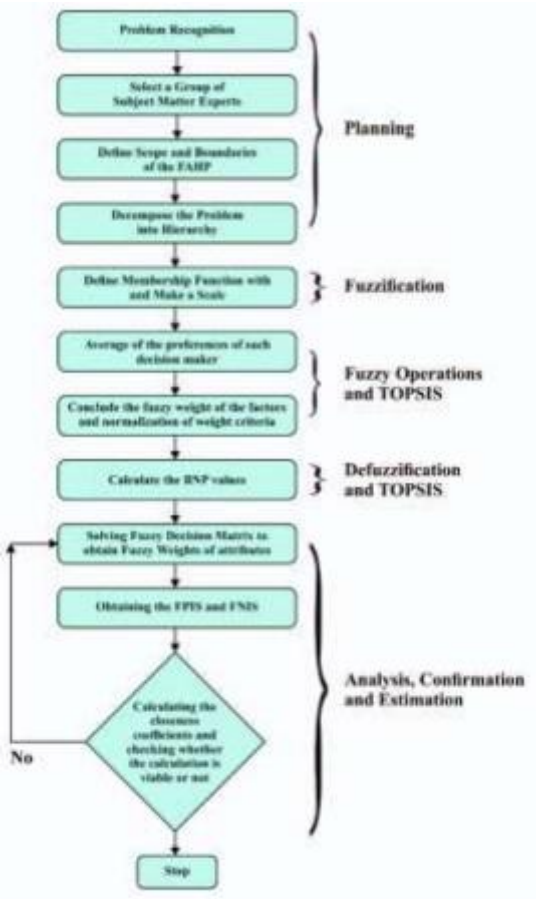


Fig1. Proposed System architecture

4. SYSTEM ARCHITECTURE



FLOW DIAGRAM:



5. CONCLUSION

Using one malicious URL, the web is crawled so as to obtain a big dataset of suspicious URLs. The suspicious URLs are retrieved using Google bot, keywords, S.E.O techniques and domain name services.

These suspicious URLs are analyzed and are declared whether they are benign or malicious, and the results are found to be mostly correct on observation.

6. OUTPUT

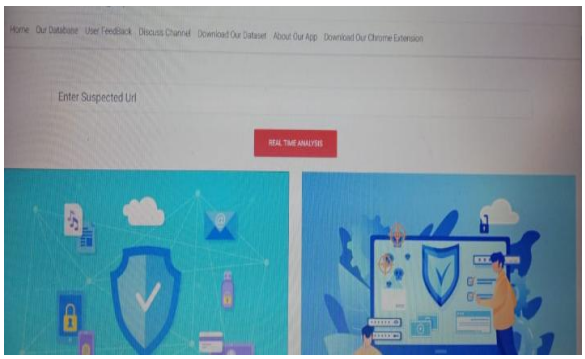


Figure 1 :Url Traffic Data

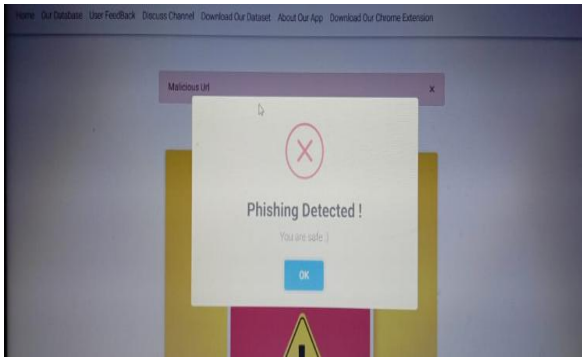


Fig 2: Malicious Web Analysis

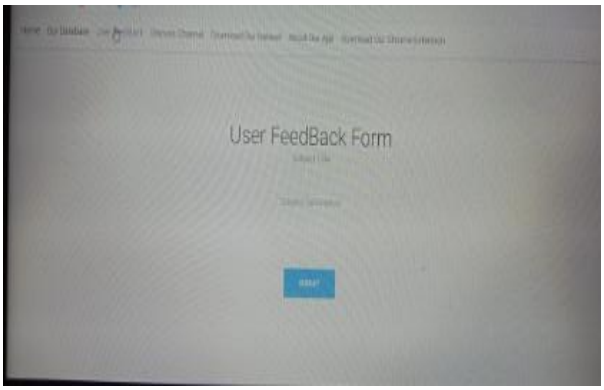


Fig 3: User Ranking feedback

REFERENCES:

[1] Ansari, M. T. J., Pandey, D., &Alenezi, M. (2018). STORE: Security threat oriented requirements engineering methodology. Journal of King Saud University-Computer and Information Sciences.

[2] Liu, J., Xiao, Y., Ghaboosi, K., Deng, H., & Zhang, J. (2009). Botnet: classification, attacks, detection, tracing, and preventive measures. EURASIP journal on wireless communications and networking, 2009(1), 692654.

[3] Peng, T., Leckie, C., &Ramamohanarao, K. (2003, May). Protection from distributed denial of service attacks using historybased IP filtering. In IEEE International Conference on Communications, 2003. ICC'03. (Vol. 1, pp. 482-486). IEEE.

[4] Boukhtouta, A., Lakhdari, N. E., Mokhov, S. A., &Debbabi, M. (2013, June). Towards Fingerprinting Malicious Traffic. In ANT/SEIT (pp. 548-555).

[5] Saha, B., &Gairola, A. (2005). Botnet: An Overivew. CERT-In White Paper. CIWP-2005-05, June.

[6] Shin, D. H., An, K. K., Choi, S. C., & Choi, H. K. (2016). Malicious traffic detection using K-means. The Journal of Korean Institute of Communications and Information Sciences, 41(2), 277-284.

[7] Bischof, H., Leonardis, A., &Selb, A. (1999). MDL principle for robust vector quantisation. Pattern Analysis & Applications, 2(1), 59-72.

[8] Kazachkin, D. S., &Gamayunov, D. Y. (2008). Network traffic analysis optimization for signature-based intrusion detection systems. In Proceedings of the Spring/Summer Young Researchers' Colloquium on Software Engineering (No. 2).

[9] Chen, T. M. (2013). Guarding against network intrusions. In Computer and information security handbook (pp. 149-163). Morgan Kaufmann

[10] Andress, J. (2014). The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Syngress.

[11] Burton, J. D. (2003). Cisco security professional's guide to secure intrusion detection systems. SyngressPubl..

[12] Lee, W., Stolfo, S. J., Chan, P. K., Eskin, E., Fan, W., Miller, M., ...& Zhang, J. (2001, June). Real time data mining-based intrusion detection. In

Proceedings DARPA Information Survivability Conference and Exposition II. DISCEX'01 (Vol. 1, pp. 89-100). IEEE.

[13] Duque, S., & bin Omar, M. N. (2015). Using data mining algorithms for developing a model for intrusion detection system (IDS). Procedia Computer Science, 61, 46-51.

[14] Bace, R. G., &Mell, P. (2001). Intrusion detection systems.

[15] Alparslan, E., Karahoca, A., &Karahoca, D. (2012). BotNet detection: Enhancing analysis by using data mining techniques. Advances in Data Mining Knowledge Discovery and Applications, 349