# Malicious URL Detector Using Convolution Neural networks

**Indra G[1], Banupriya P[2], Divya P S[3], Keerthana S[4]**
[1]Assistant professor, Dept of computer science engineering
[2, 3, 4]Dept of computer science engineering
[1, 2, 3, 4] RMK College of Engineering and Technology

***Abstract-*** *The discrimination of ordinary and malicious activity of program by monitoring URL visitors is fitting more difficult when sophisticated malware generate authorized URL traffic and having the identical habits with ordinary application. In this paper, a brand new strategy is proposed to support administrator in detection of malicious clients by using clustering customers into businesses founded on URL-pastime similarity. Size of the auto-application activity in the network can also be noticeable from the influence of the system. Nevertheless, the approach wishes to be increased for mechanically discover malicious agencies without using blacklist or outcomes of alternative malicious detection methods. One more terrible point of this system is that with a malware has simply been infected with just one client, that malware's conduct are not able to be detected. Also the identical time, the normal supervised learning algorithms are recognized to generalize well over the certain patterns determined in coaching knowledge, which makes them a greater replacement towards hacking campaigns. Nevertheless, the particularly dynamic environment of those campaigns required updating the items often, and this poses new challenges in view that many of the traditional learning algorithms are also computationally high-priced to retain.*

## I. INTRODUCTION

It has brought a great convenience to people's life since the birth of the internet.People can easily realize online shopping, learning, working, and other requirements by entering different URL in the address bar. According to we are social released "A Digital Report in 2016"data, the global internet users reached about 3.42 billion by 2016,up by 10% from 2015. The lawbreakers have seen the unlimited potential internet market. Add to interest driven, a large number of phishing attacks come into being. As phishing websites wantonly spread on the internet, the security problems of the network are becoming increasingly serious.

According to APWG (2017) (Anti-Phishing Working Group) released "Global Phishing Survey for 2016" data, there were at least 255,065 unique phishing attacks worldwide, This represented an increase of over 10% on the 230,280 received in 2015. Phishing is the malicious practice of luring you into disclosing your personal information, such as credit card number, bank account, user name and password. These phishing attacks not only bring a great loss of property to netizen, but also bring loss the reputation of enterprises. Report by Ponemon (NSFOCUS 2017) suggested that the corporation was losing on the average $ 3.7 million for a successful phishing attack in the first quarter of 2016. The investigation of Ponemon institution showed that 31 % of respondents terminated the partnership if they were told cooperative enterprise had experienced intrusion events. The harm of phishing attacks inspires scholar to pay more attention to phishing detection to avoid the unexpected attack. Since most of these phishing attacks would establish a fake website to get the victims' sensitive information, many detection technique aims at websites detection.

In recent years, as an important non-linear model for machine learning and deep learning, neural network has been successfully used in pattern recognition, data mining, and system recognition. Mohammad et al. (2014) pointed out that neural network had the advantages of nonlinearity, adaptive, generalization and fault tolerance. However, it is well knownthat neural network has the problem of over- fitting. Over-fitting is the established model achieve good performance on the training dataset, while achieve bad performance on the testing dataset. On the other hand, although there are many new detection methods for detecting phishing websites these methods cannot get desired accuracy. Therefore, the aim of this paper is to propose novel neural network model with high accuracy and good generalization ability for detecting phishing websites. Malicious URLs are intended for malicious purposes. Malicious URL or malicious website, is a common and serious threat to cyber security. A Malicious URL or a malicious web site hosts a variety of unsolicited content in the form of spam, phishing in order to launch attacks. Unsuspecting users visit such web sites and become victims of various types of scams, including monetary loss, theft of private information (identity, credit-cards, etc.). According to the latest Google Safe browsing report, Google search blacklisted over 50,000 malware sites and over 90,000 phishing sites monthly. The human understandable URLs are used to identify billions of websites hosted over the present day internet. Adversaries who try to get unauthorized access to

the confidential data may use malicious URLs and present it as a legitimate URL to naive user. Such URLs that act as a gateway for the unsolicited activities are called as malicious URLs. These malicious URLs can cause unethical activities such as theft of private and confidential data, ransom ware installation on the user devices that result in huge loss every year globally. With the advancement of social networking platforms, many allow its users to publish the unauthorized URLs.

Many of these URLs are related to the promotion of business and self-advertisement, but some of these unprecedented resource locators can pose a vulnerable threat to the naive users. The naive users who use the malicious URLs, are going to face serious security threats initiated by the adversary. The verification of URLs is very essential in order to ensure that user should be prevented from visiting malicious websites. Many mechanisms have been proposed to detect the malicious URLs. One of the basic feature that a mechanism should possess is to allow the benign URLs that are requested by the client and prevent the malicious URLs before reaching the user. This is achieved by notifying the user that it was a malicious website and a caution should be exercised. To achieve this, a system should take semantic and lexical properties of every URL rather than relying on syntactic properties of the URLs.

**I.A. NON-MACHINE LEARNING APPROACH**

Techniques such as Black – Listing, Heuristic Classification etc. comes under Non Machine Learning approach. These traditional mechanisms rely on keyword matching and URL syntax matching. Therefore, these conventional mechanisms cannot effectively deal with the ever evolving technologies and web access techniques. Furthermore, these approaches also fall short in detecting the modern URLs such as short URLs, dark web URLs. While URL blacklisting has been effective to some extent, it is rather easy for an attacker to deceive the system by slightly modifying one or more components of the URL string. Inevitably, many malicious sites are not blacklisted either because they are too recent or were never or incorrectly evaluated.

One of the collaborative work has been initiated by the top tier Internet companies such as Google, Facebook along with many of the start – up companies to build a single platform that works all together for one cause of preventing the naive users from the malicious URLs. Many of these web-based companies use exhaustive data bases which can store as many as millions of URLs, and refine these URL sets regularly. But this is not the feasible solution to all the problems. Despite having the greater accuracy, the need for human intervention to update and maintain the URL list is one of the major limiting factors in this method.

**I.B MACHINE LEARNING APPROACH**

Machine learning techniques are used to classify malicious websites through features taken from URLs web content and network activity. Machine Learning approaches, use a set of URLs as training data, and based on the statistical properties, learn a prediction function to classify a URL as malicious or benign. This gives them the ability to generalize to new URLs unlike blacklisting methods. The primary requirement for training a machine learning model is the presence of training data. In the context of malicious URL detection, this would correspond to a set of large number of URLs. Machine learning can broadly be classified into supervised, unsupervised, and semi-supervised, which correspond to having the labels for the training data, not having the labels, and having labels for limited fraction of training data, respectively. Labels correspond to the knowledge that a URL is malicious or benign. After the training data is collected, the next step is to extract informative features such that they sufficiently describe the URL and at the same time, they can be interpreted mathematically by machine learning models. For example, simply using the URL string directly may not allow us to learn a good prediction model (which in some extreme cases may reduce the prediction model to a blacklist method). Thus, one would need to extract suitable features based on some principles or heuristics to obtain a good feature representation of the URL. This may include lexical features (statistical properties of the URL string, bag of words, n-gram, etc.), host-based features (WHOIS info, geo – location properties of the host, etc.), etc.The detection methods and tools which adopt the approach of patrolling web content may consume more computation time and resource. Therefore, URL based detection techniques for malicious URL detection are largely limited to classification of URLs in general or any specific attack i.e. spam [3, 6, 20]. Meanwhile research shows that the characteristics of malicious URLs differ with the type of technique used for exploitation (e.g., spam, adware, phishing, drive-by-downloads etc.)

The features after being extracted have to be processed into a suitable format (e.g. a numerical vector), such that they can be plugged into an off – the – self machine learning method for model training. The ability of these features to provide relevant information is critical to subsequent machine learning, as the underlying assumption of machine learning (classification) models is that feature representations of the malicious and benign URLs have

different distributions. Therefore, the quality of feature representation of the URLs is critical to the quality of the resulting malicious URL predictive model learned by machine learning.

In this paper we adapted machine learning techniques to the detection and categorization of the malicious URLs. We will use CNN in order to detect whether the given URL is malicious or benign. Identification of attack types is also useful since the knowledge of the nature of a potential threat allows us to take a proper reaction as well as a pertinent and effective countermeasure against the threat. For example, we may conveniently ignore spamming but should respond immediately to malware infection.

## II. EXISTING SYSTEM

Large scrutiny has been finished in the globe of computer security for the detection of understood and unfamiliar malware maintaining disparate contraption discovering and data excavating systems. The authors utilized two static features eliminated from malware and benign multimedia, purpose size Frequency (FLF) and Printable Thread information (PSI). This work was once instituted on the hypothesis that "though aim calls and strings are self-governing of each single solitary supplementary authors underpin every single solitary supplementary in categorizing malware". Printable Thread information in every single solitary unpacked malware used to be removed and all the strings for all malware have been joined to craft a database.

***Disadvantages:***

1. Existing techniques do not account for new mobile threats such as known fraud phone numbers.
2. DNS based mechanisms do not provide deeper understanding of the specific activity implementation by a webpage or domain.
3. Existing techniques using static features of desktop webpages to detect malicious behaviors do not work well for mobile specific pages

## III. PROPOSED SYSTEM

We are basically going to use classification methods to classify a given URL as the malicious or benign. In this system, the URL is the input to the Database. Then, when the URL is input to Blacklist, we have two cases:

**Case 1:** Where the URL already exists in our blacklist, the URL will be qualified as malicious.

**Case 2:** The Feature Extraction of the URL is extracted for the analysis.

The outputs of the classifier is malicious or benign.

The architecture of the proposed system is given in the below figure. The components are World Wide Web, URL Database, Blacklist, Feature Extraction, CNN Classifier and Results.

***Advantages:***

1. This is fast and reliable static analysis technique which detects malicious URL easy GUI.

2. It provides 90% accuracy in classification, and detects a number of malicious URL in the wild that are not detected by existing techniques such as Google Safe Browsing and Virus Total.

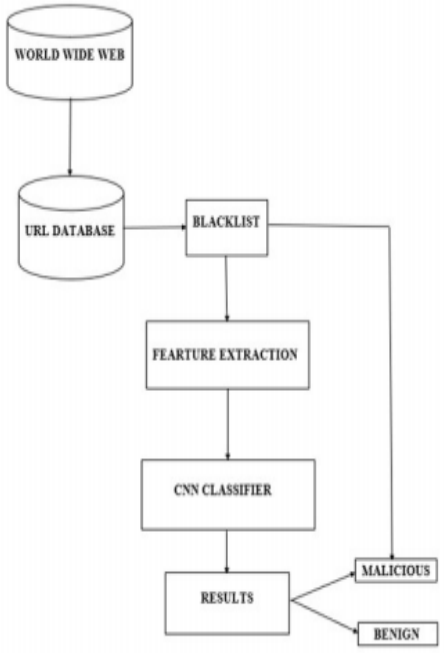


Fig 1

## IV. SYSTEM ARCHITECTURE

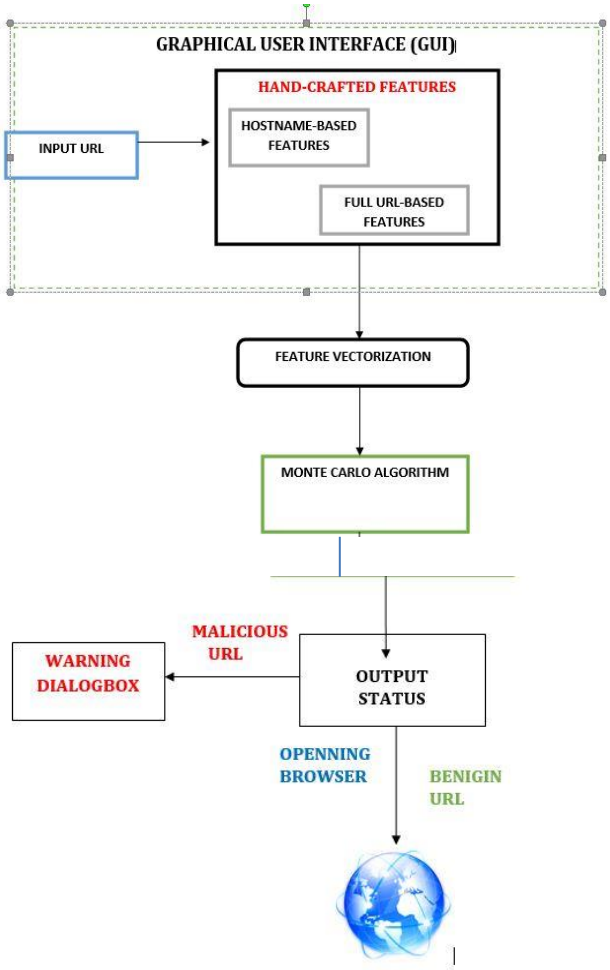


Fig 2

## V. PROJECT MODULES

*Input URL:*URL as passed as input

*Feature Extraction***:** We extracted features about the URL of the pages and composed feature matrix

*Feature vectorization:*the process of rewriting a loop so that instead of processing a single element

*Classifiers:*Classification done using Random forest classifier

*Output*: will be shown whether URL is benign or not

## VI. MODULES DESCRIPTION

*WWW / URL DATABASE:* WWW or URL database is a component from where number of URLs are fetched. These URLs from multiple websites are collected using the web crawler and are stored in the URL database.

*FEATURE EXTRACTION:* This component is used to extract the features from the URL. If the URL already exists in the blacklist then it is qualified as a malicious. In this component it will classify the URL also on the basis of lexical features.

*CNN CLASSIFIER:* This component is used to classify the URL whether it is a malicious or benign. It is done on the basis of features collected by the previous component. Previous component's result will serve as an input to this component. After the classification, the URLs will be classified as whether it is malicious or benign.

## VII. CONCLUSION

Malicious URL detection plays a critical role for many cyber security applications, and clearly deep learning approaches are a promising direction. In this article, the support vector machine algorithm based on Term frequency – inverse document frequency is compared with the logistic regression algorithm and the CNN algorithm based on the word2vac feature. By comparing the three aspects (precision, recall, and f1 –score) of SVM, logical regression and CNN, we can get a conclusion. The use of Term frequency–inverse document frequency of SVM with logical regression method, SVM of these three aspects (precision, recall, and f1 – score) are slightly higher than the logical regression algorithm. The convolution neural network based on Word2vac is consistent with the SVM algorithm based on Term frequency–inverse document frequency.

## REFERENCES

[1] Abdi, F. D., & Wenjuan, L. MALICIOUS URL DETECTION USING CONVOLUTIONAL NEURAL NETWORK.

[2] Immadisetti Naga Venkata Durga Naveen, Manamohana K, Rohit Verma DETECTION OF MALICIOUS URLS USING MACHINE LEARNING TECHNIQUES

[3] Mamun, M. S. I., Rathore, M. A., Lashkari, A. H., Stakhanova, N., & Ghorbani, A. A. (2016, September). Detecting malicious URLs using lexical analysis. In International Conference on Network and System Security (pp. 467-482). Springer, Cham.

[4] Sahoo, D., Liu, C., & Hoi, S. C. (2017). Malicious URL detection using machine learning: a survey. ArXiv preprint arXiv: 1701.07179.

[5] Thakur, S., Meenakshi, E., & Priya, A. (2017, May). Detection of malicious URLs in big data using RIPPER algorithm. In 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information &

Communication Technology (RTEICT) (pp. 1296-1301). IEEE.

[6] Vanhoenshoven, F., Nápoles, G., Falcon, R., Vanhoof, K., & Köppen, M. (2016, December). Detecting malicious URLs using machine learning techniques. In 2016 IEEE Symposium Series on Computational Intelligence (SSCI) (pp. 1-8). IEEE.