IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# MALICIOUS URL DETECTION USING 1D CNN AND TENSORFLOW JS

[1]Mr.Harish S, [2]Ms.Veni Priya T, [3]Mr.Suraj B, [4]Mr.Venkataramanan M

[1]UG Student, [2]Assistant Professor, [3]UG Student,[4]UG Student
[1]Department of Computer Science and Engineering,
[1]Arasu Engineering College, Kumbakonam, Tamil Nadu, India

***Abstract:*** Phishing web sites have been a serious chance to cyber safety which employs each social engineering and technical trick to steal clients' non-public identity statistics and monetary account information. Recent years have proved the hasty increase of phishing attacks. Phish recognizer is targeted on getting rid of the identity robbery and fraud that result from the growing problem of phishing. We propose phish recognizer, a deep learning based method which uses 1D CNN to build accurate function representation of URLs, which we use to teach a phishing URL classifier.In conclusion, the model that has been trained has a high precision and recall value and the model is converted to tensorflowJS model to run inside a browser extension.

***Index Terms*** **- 1D CNN, URL, browser extension, machine learning, phishing websites, neural network,deep learning, tensorflowJS.**

## I.INTRODUCTION

Cyber security is the agency and series of assets, methods and systems used to shield cyberspace and cyberspace enabled systems from events that misrelate through default possession rights. Cyber safety is the build-up of equipment along with regulations, security safeguards, education, chance management techniques guarantee and technology that may be used to protect the cyber organisation and environment. Because of the giant increase inside the wide variety of net users, lots of our everyday life operations are transferred from the real international to the cyber international which includes communique, coordination, trade, banking, registrations, packages, and many others. Due to this, the malicious peoples and attackers also transferred to this international and make their threats and crimes effortlessly anonymous. To make sure the safety and privacy of cyber statistics, era need to be used and prepared carefully with the aid of the use of Cyber safety. Cyber protection prevents fraud or thief who wants to seize person/public/countrywide information or connection, "identification robbery" or especially "phishing" is one of the maximum threatening safety deficits of the users within the internet. On this form of crimes, attackers use a few malicious net pages which impersonate as valid web websites, to collect the victims' critical records consisting of username, passwords, monetary data, and many others. Usually, a phishing attack starts with an e-mail which appears to return from a good enterprise as depicted in safety problems. The content of the mail encourages the victim to click on the cope with, which can also be hidden as a hypertext. This address directs the sufferer to a fake web website online, which is designed exactly similar to a valid internet site, together with an e-mail web page social engineering site of normally financial institutions web websites. To overcome this form of attack there is need to construct a dynamic and green algorithm that could learn the shape of the valid web pages and classify the strange ones. Therefore, on this mission, we aimed to set up a classification system that can discover whether or not an URL is both phishing or legitimate. examine the efficiency of the one of a kind algorithms and select the quality one,We used Classical Machine learning algorithms and deep learning methodologies. experimental consequences showed that the proposed methods produce superb accuracy for detecting phishing URLs. Phishing is a criminal mechanism which employs both social engineering and technical subterfuge to borrow customers' personal identification data and financial account facts.

Implementation of a machine which accrued many respectable and phishing URLs. With the amassed dataset, the authors evaluated and in comparison various classification algorithms which includes choice Decision Tree (DT), Naive Bayes (NB), and Neural Networks (NN), deep studying technique. The details of our method to URL classification are discussed in Sect. 3 the writer affords the assessment results via lots of classification algorithms. Section 8 is the conclusion of this paper.

## II. RELATED WORKS

Several research papers tackled the problem of detecting malicious URLs. The recent work of [13] presented a survey covering this topic. The authors presented up-to-date approaches implemented to protect users from malicious sites. Detection of false URLs may fall under one of two categories as discussed in the following subsections. A. List based detection systems All approaches under this category used two kinds of lists; a whitelist and a blacklist. Both lists are used to classify URL links to be either malicious or legitimate. URLs not listed in the whitelist are considered False ones. In [8], the authors proposed a software system using a whitelist made of IP addresses of legitimate websites where users are notified when visiting unlisted websites. In [14], the authors proposed a dynamic whitelist which is updated automatically. Their approach is made of two steps: (i) IP address matching, and (ii) Features extraction from URL text pieces. Experimental results showed great performance in protecting internet users from false URLs. Blacklists are created to manage URLs. Usually, a blacklist is deployed as a key element in anti-virus, security software systems and spam detection systems. The main advantage of a blacklist is to prevent hackers from using the same URL or IP address again. However, a blacklist may not prevent a first time attack with a new URL or an IP address. The percentage rate of success of the blacklist approach may not exceed 20% [15], [16]. Several companies such as Google Safe Browsing API and PhishNet provide a blacklist service. However, the blacklist needs frequent updates and requires excessive system resources [17]. In [18], the authors used a simple algorithm to detect and predict whether URLs are legitimate or phishing. First a URL is checked against a blacklist database. If the URL is already in the blacklist it is classified as malicious. If it is not found, then the features of the URL are extracted for further analysis. A simple classifier is used to predict if the URL is malicious or benign. B. Machine learning based detection systems Machine learning (ML) approaches have been applied successfully to detect false URL links. ML looks to this problem as a classification problem. Learning algorithms should be trained using good enough samples of True/False URLs to build accurate models for online detection. In [19], the authors proposed a text-based detection approach which extracted words from URL links and searched for these words using Google search engine. If the URL text is detected in the search results, it will be considered as a true URL otherwise it will be a false one. In [20], the authors applied an adaptive self-structuring neural network for the classification of true and false URLs. The authors in [21] applied a natural language processing (NLP) approach. They have a feature vector of 209 words and 17 NLP based features. In [22], the authors proposed an event denoising convolutional neural network (EDCNN) system for detecting malicious URL sequences from proxy logs. They used EDCNN to reduce the negative effect of benign URLs redirected from compromised websites included in malicious URL sequences. Their evaluation showed that the EDCNN lowers the operation cost of malware infection by reducing 47% of false alerts compared with a CNN when users access compromised websites but do not obtain exploit code due to browser fingerprinting. In [23], the authors applied a nonlinear regression strategy for detecting whether a website is true or not. They used a hybrid approach based on harmony search (HS) and support vector machine (SVM) for the training process. The authors of [24] applied natural language processing to detect false emails. The proposed approach applied semantic analysis on the content of emails using a predetermined blacklist. In this paper, we propose a 1d convolutional neural network (CNN-1D) model to detect Malicious URLs. We evaluate the performance of our model using a benchmarked dataset and two evaluation measures: accuracy and AUC.

### A. DEEP LEARNING BASED DETECTION:

To deal with the aforementioned defects, a few deep learning primarily based phishing website detection solutions have these days come to light due to the success in herbal Language Processing (NLP) executed by way of deep learning. Some researchers focused on detecting phishing URLs by leveraging the characteristics of URLs. In comparison, different studies absolutely exploited content material-based features or occasion-primarily based capabilities for phishing web sites detection. The formerly noted deep gaining knowledge of based totally ones is that we combine the benefits of CNN and attention-based hierarchical RNN to extract novel individual degree spatial and word-degree temporal characteristic representations of URLs automatically, which become conducive to the improvement of phishing detection various performance.

## III. PROPOSED SYSTEM

The Proposed algorithm is primarily based on a computerized real-time phishing detection and advice mastering procedure. The phishing URLs in most cases have a couple of connections among the part of the URL which means an inter-relatedness and with the aid of the use of it the capabilities of phishing URLs are extracted. Then the extracted capabilities are used for a device-gaining knowledge of class to come across Phishing websites on actual time. The characteristics of phishing web sites which used to differentiate from legitimate websites. The values are then assigned to each phishing indicator with the variety defined for phishing website risk. The URLs are pre-processed for the tokenization process. The pre-processed dataset is used to extract the sub domain,domain and domain suffix.

The data set is composed of 420264 phishing websites collected from various sources.

## IV. APPROACH AND IMPLEMENTATION

This section has focused on implementation of a crawler, and uses it to analyse the URL and its website content to extract the characteristics. URLs are separated into 2 classes:

*(a)* ***Legitimate:*** *URL is safe and the website provides normal services.*

*(b)* ***Phishing:*** *Website performs unintended actions to get sensitive data of its users such as email, password, and credit card details by tricking users to enter their personal information into a form.*

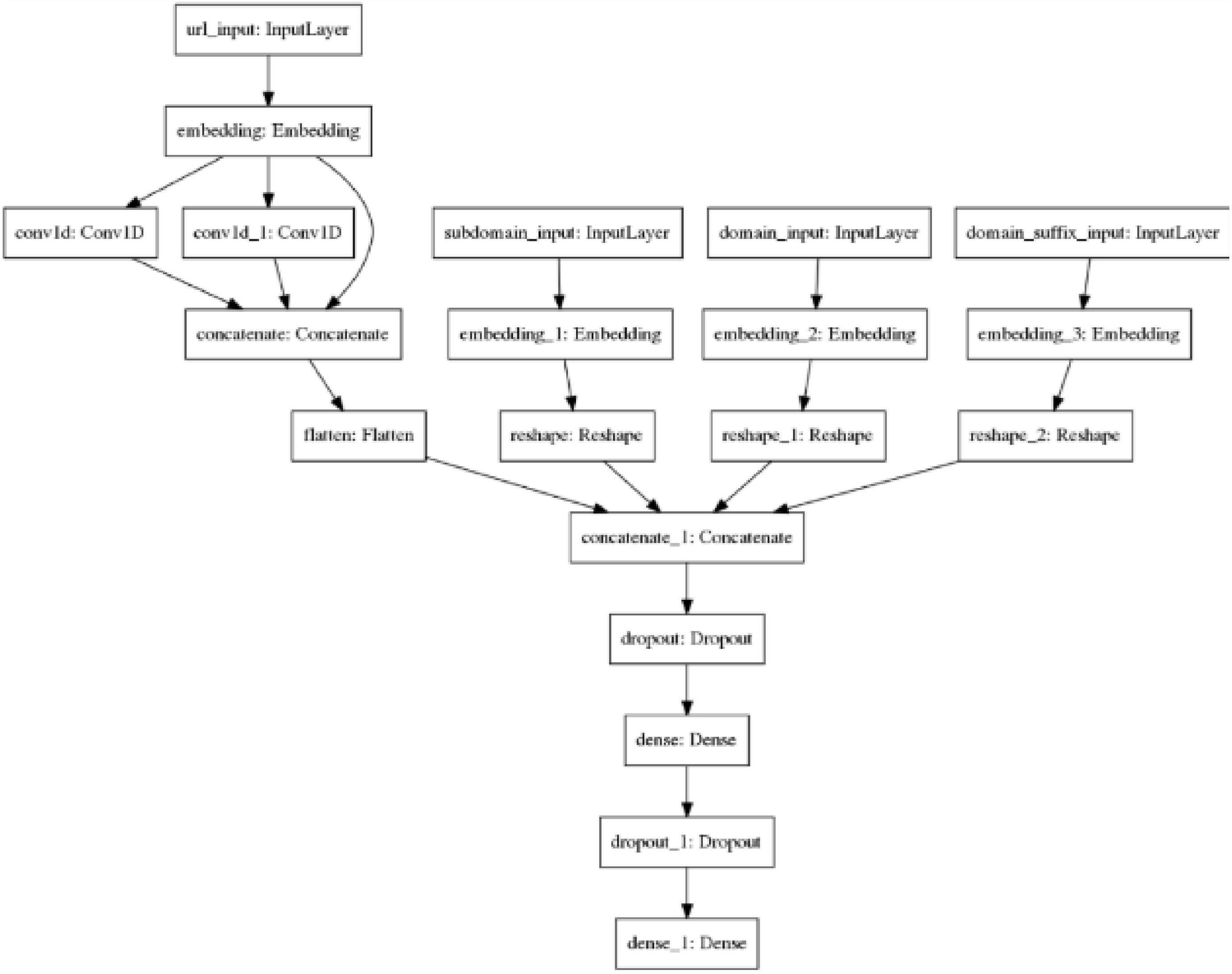
### 4.1 .URLs

The name of the web page in the html form. Within the well-known shape, a URL starts with its protocol call, such as hypertext transfer protocols, file transfer protocols, etc., which are used to get right of entry to the net page. Therefore, the subdomain and the second one degree area (SLD) names perceive the server hosting the net website online. SLD names could be very essential for us, due to the fact this element mainly incorporates the call of the firm, therefore, phishers focussed on this element and try to produce different sorts of names which are like unique ones. The pinnacle-degree domain (TLD) name indicates the domains within the area name machine root quarter of the net inclusive of educational, industrial government, and so on. Finally, the Geographical area call shows the geographical place of the internet web site consisting of Germany, Turkey, France, and many others. The preceding four elements compose the area call (host name) of the net web page; however, the internal deal with is represented by way of the route of the page within the server and with ongoing component is like a folder a file call which suggests the vicinity of the file inside the server.

### 4.2. TRAINING THE SYSTEM

One of the most successful approaches recently used in the classification problems is the Convolutional Neural Network (CNN). CNN is used for complex hard classification problems [25].

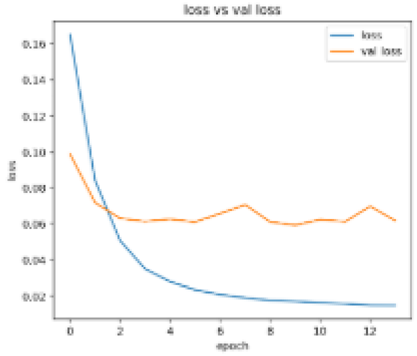
More specifically, CNN is used in the image processing domain [26]. In this paper, we implemented a CNN-1D model using Keras with a TensorFlow- GPU backend technique to tackle the problem of detecting false URLs. The main concept of CNN is quite similar to linear neural network, which takes raw data as an input (1D vector). The first convolutional layer has 64 filters with kernel size of 3 and The second convolutional layer has 64 filters with kernel size of 5 ReLU activation followed by a concatenate layer. The subdomain,domain and domain suffix are passed into the embedding layer followed by a dropout layer. The final layer is a dense layer with one neuron,

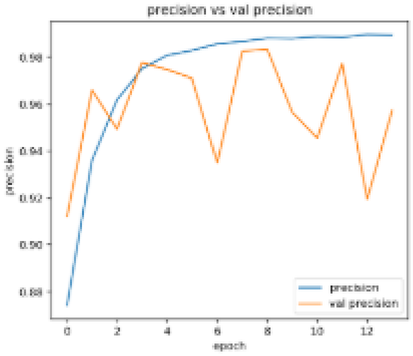


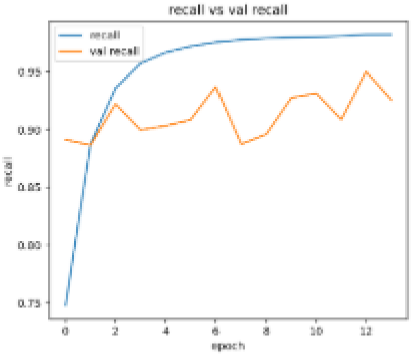
allowing the complete model to output binary classifications (i.e a Malicious or legitimate URL). Figure above shows the architecture of the CNN-1D model used in this work.

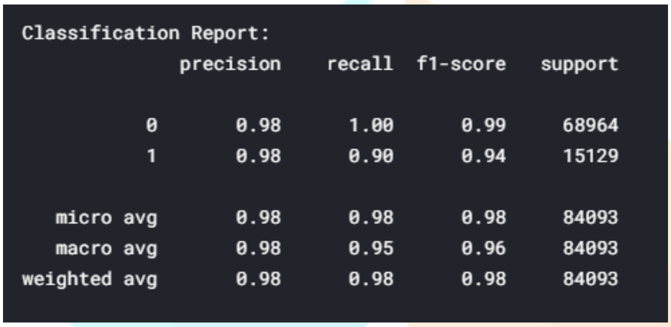
## V. Results and Discussion

The model that has been trained has a high precision and recall value but what must be considered is the precision value. The precision value must be high because if it is low then a website that is not malicious has the possibility to be classified as malicious.









```
Classification Report:
              precision    recall  f1-score   support

           0       0.98      1.00      0.99     68964
           1       0.98      0.90      0.94     15129

   micro avg       0.98      0.98      0.98     84093
   macro avg       0.98      0.95      0.96     84093
weighted avg       0.98      0.98      0.98     84093
```

## VI. Conclusion

Protecting internet users from faked URLs is in high demand. Fraudsters by all means attempt to steal sensitive information from users through faked URL links. Novice and inattentive internet users are always the best targets for this malicious action and many have been falling in this trap. In this work, we introduced the deep learning CNN-1D model to predict malicious/legitimate URLs to protect internet users from attacks. We carried out a few experiments to evaluate the proposed model using a benchmarked dataset. We used two evaluation measures, namely, accuracy and area under the curve (AUC). The CNN-1D model was able to achieve good performance for predicting the status of the unseen URLs. The accuracy rate for testing was 97.85% and the keras model was converted to tensorflow JS model. In addition, the proposed approach was also good in terms of the AUC scale for both training and testing instances. For future work we plan to investigate the design and implementation of an adaptive CNN-1D model to handle the problem of faked URLs using tensorflowJS which can be run on the browser itself.

## References

**[1]** K. Greene, M. Steves, and M. Theofanos, "No phishing beyond this point," Computer, vol. 51, no. 6, pp. 86–89, June 2018.

**[2]** F. Michclinakis, H. Doroud, A. Razaghpanah, A. Lutu, N. VallinaRodriguez, P. Gill, and J. Widmer, "The cloud that runs the mobile internet: A measurement study of mobile cloud services," in IEEE INFOCOM 2018 - IEEE Conference on Computer Communications, 2018, pp. 1619–1627.

**[3]** K. Sha, W. Wei, T. A. Yang, Z. Wang, and W. Shi, "On security challenges and open issues in the internet of things," Future Generation Computer Systems, vol. 83, pp. 326 – 337, 2018.

**[4]** K. Rajitha and D. Vijayalakshmi, "Suspicious urls filtering using optimal rt-pfl: A novel feature selection based web url detection," in Smart Computing and Informatics, S. C. Satapathy, V. Bhateja, and S. Das, Eds. Singapore: Springer Singapore, 2018, pp. 227–235.

**[5]** S. Kim, J. Kim, and B. B. Kang, "Malicious url protection based on attackers' habitual behavioral analysis," Computers Security, vol. 77, pp. 790 – 806, 2018.

**[6]** K. Thomas, C. Grier, D. Song, and V. Paxson, "Suspended accounts in retrospect: An analysis of twitter spam," in Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference, ser. IMC '11. New York, NY, USA: ACM, 2011, pp. 243–258.

**[7]** M. Volkamer, K. Renaud, B. Reinheimer, and A. Kunz, "User experiences of torpedo: Tooltip-powered phishing email detection," Computers Security, vol. 71, pp. 100 – 113, 2017.

**[8]** Y. Cao, W. Han, and Y. Le, "Anti-phishing based on automated individual white-list," in Proceedings of the 4th ACM Workshop on Digital Identity Management, ser. DIM '08. New York, NY, USA: ACM, 2008, pp. 51–60.

**[9]** A. Y. Fu, L. Wenyin, and X. Deng, "Detecting phishing web pages with visual similarity assessment based on earth mover's distance (emd)," IEEE Transactions on Dependable and Secure Computing, vol. 3, no. 4, pp. 301–311, Oct 2006.

[10] A. Stone, "Natural-language processing for intrusion detection," Computer, vol. 40, no. 12, pp. 103–105, Dec 2007.

**[11]** D. L. Cook, V. K. Gurbani, and M. Daniluk, "Phishwish: A stateless phishing filter using minimal rules," in Financial Cryptography and Data Security, G. Tsudik, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 182–186.

**[12]** S. Abu-Nimeh, D. Nappa, X. Wang, and S. Nair, "A comparison of machine learning techniques for phishing detection," in Proceedings of the Anti-phishing Working Groups 2Nd Annual eCrime Researchers Summit, ser. eCrime '07. New York, NY, USA: ACM, 2007, pp. 60–69.

**[13]** B. B. Gupta, N. A. G. Arachchilage, and K. E. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions," Telecommunication Systems, vol. 67, no. 2, pp. 247–267, Feb 2018.

**[14]** A. K. Jain and B. B. Gupta, "A novel approach to protect against phishing attacks at client side using auto-updated white-list," EURASIP Journal on Information Security, vol. 2016, no. 1, p. 9, May 2016.

**[15]** M. Khonji, Y. Iraqi, and A. Jones, "Phishing detection: A literature survey," IEEE Communications Surveys Tutorials, vol. 15, no. 4, pp. 2091–2121, Fourth 2013.

**[16]** S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ser. CHI '10. New York, NY, USA: ACM, 2010, pp. 373–382.

**[17]** S. Sheng, B. Wardman, G. Warner, L. Cranor, J. Hong, and C. Zhang, "An Empirical Analysis of Phishing Blacklists," 7 2009.

**[18]** F. D. Abdi and L. Wenjuan, "Malicious url detection using convolutional neural network," Journal International Journal of Computer Science, Engineering and Information Technology, vol. 7, no. 6, pp. 1–8, 2017.

**[19]** Y. Zhang, J. I. Hong, and L. F. Cranor, "Cantina: A content-based approach to detecting phishing web sites," in In Proceedings of the 16th International Conference on World Wide Web, WWW '07, ACM, New York, NY, USA, 2007, p. 639–648.

**[20]** R. M. Mohammad, F. Thabtah, and L. McCluskey, "Predicting phishing websites based on self-structuring neural network," Neural Computing and Applications, vol. 25, no. 2, pp. 443–458, Aug 2014.

**[21]** E. Buber, B. Dırı, and O. K. Sahingoz, "Detecting phishing attacks from url by using nlp techniques," in 2017 International Conference on Computer Science and Engineering (UBMK), Oct 2017, pp. 337–342.

**[22]** T. Shibahara, K. Yamanishi, Y. Takata, D. Chiba, M. Akiyama, T. Yagi, Y. Ohsita, and M. Murata, "Malicious url sequence detection using event denoising convolutional neural network," in 2017 IEEE International Conference on Communications (ICC). IEEE, 2017, pp. 1–7.

**[23]** M. Babagoli, M. P. Aghababa, and V. Solouk, "Heuristic nonlinear regression strategy for detecting phishing websites," Soft Computing, Feb 2018.

**[24]** T. Peng, I. Harris, and Y. Sawa, "Detecting phishing attacks using natural language processing and machine learning," in 2018 IEEE 12th International Conference on Semantic Computing (ICSC), Jan 2018, pp. 300–301.