Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 3, March : 2025

PHISHING WEBSITE DETECTION USING LSTM NETWORKS: A DEEP LEARNING APPROACH

Dr. D. P. V. Phani Raja Kumar Department of Computer Science Seshadri Rao Gudlavalleru Engineering College (Affiliated to JNTUK) Gudlavalleru, India phanisrrcs@gmail.com
Ragi Varsha, Puvvula Siva Sai Phani Suman, Madem Vineeth, Puli Eswar Reddy, Department of Computer Science Seshadri Rao Gudlavalleru Engineering College (Affiliated to JNTUK) Gudlavalleru, India varsharagi776@gmail.com

Abstract: Traditional phishing detection methods struggle to keep pace with evolving cyber threats. An LSTM-based deep learning system in order to identify fraudulent websites are presented in this study. The model effectively captures temporal dependencies and contextual patterns within webpage content, distinguishing phishing websites from legitimate ones. Additionally, an attention mechanism enhances feature extraction, improving detection accuracy. In comparison to more traditional methods, our results show significant improvements in accuracy, precision, and recall across a variety of datasets. The model's adaptability to emerging phishing strategies through continuous learning makes it a robust solution for phishing detection.
Index terms *- Phishing website detection, Deep learning, LSTM networks, Attention mechanism, Cybersecurity, Intrusion detection, Network security, Feature extraction, Machine learning, NSL-KDD dataset.*

1. INTRODUCTION

Online services are becoming indispensable due to the rapid development of Internet technology. However, along with these conveniences, cybersecurity threats such as phishing attacks, network viruses, and malicious intrusions have also increased significantly. Cybercriminals continuously evolve their tactics, making it challenging to detect fraudulent activities using traditional security measures. As a result, phishing attacks have emerged as a major concern, targeting unsuspecting users by impersonating legitimate websites to steal sensitive information.

IDS ensures network security by monitoring and analysing traffic to detect threats. Traditional IDS methods rely on pattern matching and rule-based techniques, which struggle to adapt to new and sophisticated cyberattacks. ML and DL approaches have gained prominence in intrusion detection, enabling automated and intelligent detection of malicious activities. Among these, Capturing temporal dependencies has been successfully accomplished by LSTM networks. and complex patterns in network traffic data, making them well-suited for phishing website detection.

In this study, we suggest an LSTM-based DL model to enhance phishing detection accuracy. By leveraging an extensive dataset containing both phishing and legitimate websites, our model learns intricate features and adapts to evolving phishing strategies. The addition of an attention mechanism enhances the model's capability to zero in on critical elements of online material, enhancing classification performance. By delivering a robust and scalable phishing defence, our methodology outperforms prior approaches in terms of accuracy, precision, and recall.

2. LITERATURE SURVEY

2.1 A Survey of Machine Learning-Based Solutions for Phishing Website Detection

https://www.mdpi.com/2504-4990/3/3/34

ABSTRACT: As the Internet has grown, people's interest in network security has increased. The fast and sustained spread of the Internet may have been helped by secure network settings. Phishing refers to the practice of deceiving users into clicking on malicious links in order to steal sensitive information or access connected accounts and funds. Phishing is a crucial class of cybercriminals. Attack and

defence in network security are iterative processes. Both phishing techniques and phishing detection technologies are always evolving. Blacklists and whitelists are the foundation of traditional phishing link detection techniques, however they are unable to detect newly created phishing URLs. As machine learning technology has advanced, prediction has emerged as a critical skill. This study provides a cutting-edge overview of techniques for identifying phishing websites. The phishing life cycle is covered first, followed by an introduction to popular anti-phishing techniques, an emphasis on phishing link identification, and In-depth analysis of systems that utilise machine learning, gathering information, extracting features, developing models, and assessing results. This study analyses several ways for detecting phishing websites.

2.2 A Smart Model for Web Phishing Detection Based on New Proposed Feature Selection Technique:

https://www.researchgate.net/publication/342858172_A_Smart_Model_for_Web_Phishing_Detection_Based_on_New_Proposed_Feature_Selection_Technique

ABSTRACT: One of the most dangerous types of cybercrime is web-phishing. It gives hackers access to several users' devices and allows them to eavesdrop on their personal information, including credit card numbers and passwords. Hackers employ a variety of online techniques to deceive people into sharing information, downloading files, or clicking on links that compromise a computer. This study suggests a meta-heuristic-based strategy to shield internet users against online phishing. The process is split into three parts. The first step is to evaluate the website's text, images, URL, domain name, HTML, and JavaScript code using a newly proposed method. Secondly, we get the effective subset of evaluated features that are the most accurate in classifying web phishing attempts. In the third stage, the RF classifier is built using the retrieved subset's data characteristics. The newly suggested feature selection approach produced the best classification accuracy. When compared to the adaptive Neuro-fuzzy inference system, the suggested web-phishing detection approach achieved better results in terms of classification accuracy and time.

2.3 A novel approach for phishing URLs detection using lexical based machine learning in a real-time environment:

https://www.sciencedirect.com/science/article/abs/pii/S0140366421001675

ABSTRACT: The gadgets include cloud networks, cellphones, and the Internet of Things, among others. Phishing attacks are more common on these devices than other potential cyberattacks because they take use of human weaknesses rather than technology weaknesses. Phishing attacks occur when an internet user is tricked into providing personal information, such as credit card numbers or login credentials, by an organisation that appears to be trustworthy. When hackers get access to this sensitive information, it serves as the foundation for more complex assaults. Despite using a number of characteristics to create effective phishing detection systems, researchers have recently suggested using machine learning to avoid phishing. Since phishing demands a lot of processing power and features, it cannot be detected by smartphones with lesser resources. In order to solve this problem, we have created a phishing detection method that can identify phishing assaults with just nine lexical criteria. After testing our method against other machine learning classifiers, we found that the RF technique produced the best accuracy, 99.57%.

2.4 ISHO: improved spotted hyena optimization algorithm for phishing website detection:

https://link.springer.com/article/10.1007/s11042-021-10678-6

ABSTRACT: The prevalence of fraudulent websites that steal user information is one of the main issues in cyberspace and Internet of Things (IoT) ecosystems. As a multimedia system, a website offers access to several data kinds, including text, images, audio, and video. Each of these data types is trimmed so that fishermen may use it to launch a phishing attack. People are led to phoney websites in phishing assaults, when a thief or phisher steals their personal data. The most popular algorithms for categorising webpages and identifying phishing attempts are ML and data mining techniques. The feature selection technique used to pick relevant information for classification has a significant impact

on classification accuracy. When selecting characteristics for SVM classification of phishing websites. The accuracy of ISHO was higher than that of spotted hyena optimisation. Furthermore, when compared to other meta-heuristic approaches, the ISHO technique performs better than firefly, particle swarm optimisation, and bat. Additionally, the suggested approach is contrasted with many classification algorithms that have already been proposed on the same dataset.

2.5 Efficient deep learning techniques for the detection of phishing websites

https://link.springer.com/article/10.1007/s12046-020-01392-4

ABSTRACT: Phishing is a type of cyberattack and fraudulent conduct that is carried out with the express intent of obtaining private information by impersonating legitimate websites. Phishers deceive consumers by mimicking authentic and authentic material in order to divulge personal data, including passwords, credit card numbers, security numbers, and more. Even though modern browsers have been designed to lessen the likelihood that users may become ensnared in a malicious scheme, individuals nonetheless fall victim to phishers website identification based on heuristic characteristics, and they used 18 features to reach a 99.5% accuracy rate. employing just ten features from our previous work. The accuracy of the suggested method is 99.43% for CNN, 99.52% for DNN, and 99.57% for LSTM. The suggested methods boost the speed of phishing detection and are more resilient to failure since they only use one third-party service feature.

3. METHODOLOGY

i) Proposed Work:

The proposed phishing detection system is based on a DL model utilizing LSTM networks, designed to effectively analyze and classify website content. The model is structured to capture temporal dependencies and contextual information in webpage data, enabling precise differentiation between phishing and legitimate websites.

The system consists of multiple layers, including an input layer for data preprocessing, LSTM layers for sequential feature extraction, and an attention mechanism to focus on critical elements contributing to phishing detection. The attention mechanism enhances feature selection, ensuring that the model prioritizes relevant characteristics of a webpage while filtering out irrelevant details.

To improve detection accuracy, the model is trained on a comprehensive dataset that includes a diverse range of phishing and legitimate websites. This ensures that the system adapts to new phishing strategies and remains effective against evolving threats. Results from experiments conducted on standard datasets show that the suggested LSTM-based model achieves better results than conventional detection methods with respect to recall, precision, and accuracy.

ii) System Architecture:

The proposed phishing detection system is built using a multi-layer deep learning architecture that combines LSTM networks with an attention mechanism to enhance feature extraction and classification accuracy. The system begins with an input layer, where webpage content is preprocessed and converted into a structured numerical format. This data is then fed into multiple convolutional layers, which transform the input into feature representations. The LSTM layer processes these sequential features, capturing temporal dependencies and contextual relationships crucial for phishing detection. To further improve performance, an attention mechanism is integrated, enabling the model to zero down on the essential distinctions between legitimate and fraudulent websites. At last, the output layer determines whether a website is legitimate or a phishing attempt. The design is precise, flexible, and resistant to evolving phishing techniques.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 3, March : 2025

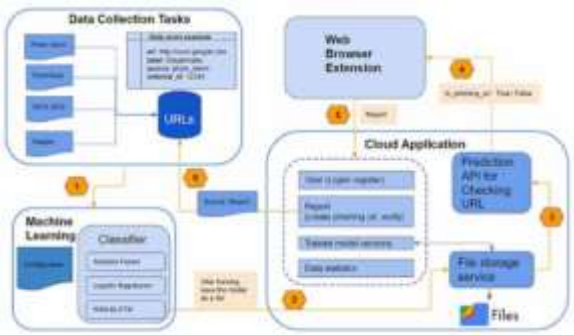

Fig 1 Proposed architecture

iii) Modules:

a) Data Preprocessing:

- Converts raw webpage content into numerical representations using text tokenization and feature extraction.
- Normalizes data to ensure consistent input for the deep learning model, improving accuracy.

b) Feature Extraction:

- Uses convolutional layers to extract meaningful patterns from webpage content.
- Captures both textual and structural features essential for phishing detection.

c) LSTM-Based Classification:

- Leverages LSTM networks to analyze sequential dependencies in webpage content.
- Enhances the ability to detect phishing attempts by learning long-range contextual relationships.

d) Attention Mechanism:

- Highlights key webpage elements that contribute significantly to phishing detection.
- Improves classification accuracy by focusing on crucial features while filtering irrelevant data.

e) Model Training and Evaluation:

- Trains the LSTM model using a diverse dataset of phishing and legitimate websites.
- Evaluates performance using metrics like accuracy, precision, recall, and F1-score.

f) Detection and Alert System:

- Classifies websites in real time, identifying phishing threats effectively.
- Generates alerts and reports for administrators to take necessary cybersecurity measures.

iv) Algorithms:

1. Recurrent Neural Network (RNN):

RNN is a neural network model designed to handle sequential data by maintaining an internal memory. Each input depends on the previous one, allowing the model to retain context across time steps. To enable sequence-based learning, the subsequent step takes the output of the current input.

The formula for the current state is:

$$h_t = f(h_{t-1}, x_t)$$

$$h_t = \tanh (W_{hh}h_{t-1} + W_{xh}x_t)$$

ht=tanh⁡(WhxXt+Whhht−1)
h_t = \tanh(W_{hx}X_t + W_{hh}h_{t-1})ht=tanh(WhxXt+Whhht−1)
where hth_tht is the hidden state, XtX_tXt is the current input, WhxW_{hx}Whx and WhhW_{hh}Whh are weights, and tanh⁡\tanhtanh is the activation function.

RNNs are widely used in applications like speech recognition, handwriting recognition, and time-series forecasting. Nevertheless, representing sequence connections throughout time becomes challenging due to fading and exploding gradients.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 3, March : 2025

2. Long Short-Term Memory (LSTM):

In order to address the vanishing gradient issue, LSTM—an upgraded RNN—uses three crucial gates:

a) Input Gate: Determines which values from the input should be stored in memory. A sigmoid function filters the input, and a tanh function assigns importance levels between -1 and 1.

b) The Forget Gate is responsible for selecting which data points from previous states to erase. A sigmoid function generates values between 0 (omit) and 1 (retain) for each memory unit.

c) Output Gate: Uses both memory content and input to determine the final output. The sigmoid function filters values, while the tanh function scales their importance before outputting the result.

LSTMs are highly effective in time-series forecasting, NLP tasks, and speech recognition due to their ability to maintain long-term dependencies. However, their complex architecture makes them computationally expensive and data-intensive.

4. EXPERIMENTAL RESULTS

Accuracy: How well a test can differentiate between healthy and sick individuals is a good indicator of its reliability. Compare the number of true positives and negatives to get the reliability of the test. Following mathematical:

Accuracy = TP + TN /(TP + TN + FP + FN)

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

Precision: The accuracy rate of a classification or number of positive cases is known as precision. Accuracy is determined by applying using the one that follows:

Precision = (TP)/ (TP + FP)

$$\text{Precision} = \frac{True\ Positive}{True\ Positive + False\ Positive}$$

Recall: The ability of a model to identify all pertinent instances of a class is assessed by machine learning recall. Looking at the ratio of expected positives to actual positives, it reveals how well a model captures examples of a class.

$$Recall = \frac{TP}{TP + FN}$$

MAP: Evaluating the level of quality Average Mean Accuracy (MAP). The position on the list and the number of pertinent recommendations are taken into account. The Mean Absolute Precision (MAP) at K is the sum of all users' or enquiries' Average Precision (AP) at K.

$$mAP = \frac{1}{n}\sum_{k=1}^{k=n} AP_k$$

$$AP_k = the\ AP\ of\ class\ k$$

$$n = the\ number\ of\ classes$$

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 3, March : 2025

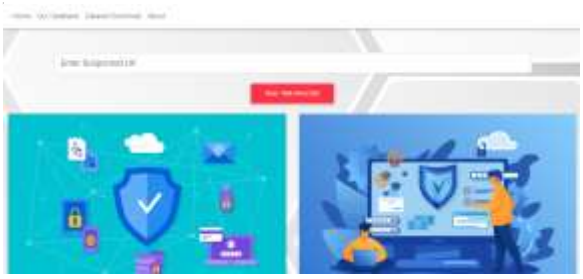

Fig 2 home page

Fig 3. results

Fig 4 Malicious URL Detected

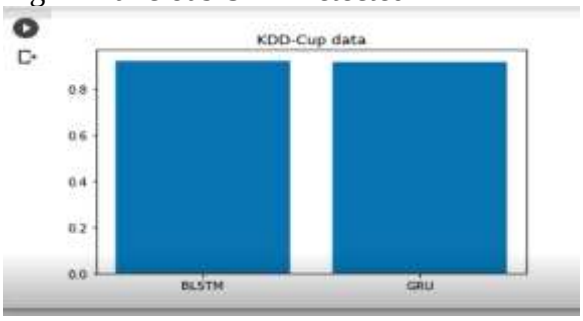

Fig 5 accuracy graph

5. CONCLUSION

We suggest the BAT-MC, a comprehensive deep learning model composed of LSTM and consideration components. The problem of interruption finding may be effectively handled by BAT-MC, which also offers an additional exploration method for interruption detection. 2) To highlight the important information, we incorporate the consideration component into the LSTM model. The component data that was obtained is accurate and logical. 3) We show that the BAT-MC model can eliminate data from each parcel when compared to standard deep learning techniques. Through the use of organisation traffic construction data, the BAT-MC model is able to capture features even more thoroughly. 4) We use an authentic NSL-KDD dataset to evaluate our suggested network. According to the test findings, BAT-MC presentation outperforms traditional techniques.

6. FUTURE SCOPE

The BAT-MC model has significant potential for further enhancements and applications in cybersecurity. To improve the model's computational efficiency for phishing in real-time, more

research is needed and intrusion detection in large-scale networks. Integrating reinforcement learning techniques with LSTM can further improve adaptive learning capabilities, allowing the model to dynamically respond to evolving cyber threats. Additionally, expanding the dataset to include more diverse and real-world phishing attack patterns can enhance the model's robustness. Implementing the BAT-MC framework in cloud-based security systems and IoT environments can also provide a scalable solution for safeguarding distributed networks.

REFERENCES

[1] B. B. Zarpelo, R. S Miani, C. T. Kawakani, and S. C. de Alvarenga, ''A survey of intrusion detection in Internet of Things,'' J. Netw. Comput. Appl., vol. 84, pp. 25–37, Apr. 2017.
[2] B. Mukherjee, L. T. Heberlein, and K. N. Levitt, ''Network intrusion detection,'' IEEE Netw., vol. 8, no. 3, pp. 26–41, May 1994.
[3] S. Kishorwagh, V. K. Pachghare, and S. R. Kolhe, ''Survey on intrusion detection system using machine learning techniques,'' Int. J. Control Automat., vol. 78, no. 16, pp. 30–37, Sep. 2013.
[4] N. Sultana, N. Chilamkurti, W. Peng, and R. Alhadad, ''Survey on SDN based network intrusion detection system using machine learning approaches,'' Peer-to-Peer Netw. Appl., vol. 12, no. 2, pp. 493–501, Mar. 2019.
[5] M. Panda, A. Abraham, S. Das, and M. R. Patra, ''Network intrusion detection system: A machine learning approach,'' Intell. Decis. Technol., vol. 5, no. 4, pp. 347–356, 2011.
[6] W. Li, P. Yi, Y. Wu, L. Pan, and J. Li, ''A new intrusion detection system based on KNN classification algorithm in wireless sensor network,'' J. Electr. Comput. Eng., vol. 2014, pp. 1–8, Jun. 2014.