IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

PHISNETGUARD: A Real-Time Phishing Website Detection Model

A review

[1]Mukesh Raj, [2]Vansh Vikram Singh, [3]Trishala Singh, [4]Srishti Sharan, [5]Ajay Kumar Singh

[1]Assistant Teacher, [2]Student, [3]Student, [4]Student, [5]Student

[1]Computer Science Engineering,

[1]JSS Academy of Technical Education, Noida, UP, India

Abstract:

Among all sorts of cybercrimes, Phishing is one of the most common and menacing, where the scammers make the users reveal sensitive data like users' login credentials, personal details, and financial information by forcing users to trust that they are legitimate organizations such as banks or popular websites. Being the most integrated part of our lives, the internet is still the primary source of evolving phishing attacks, which are difficult to identify. New rapidly changing phishing attacks break through traditional security system measures such as blacklists or heuristic-based detection methods. These methods cannot adapt quickly to recognize threats, leaving individuals and organizations to significant data breaches. The Internet is an essential platform in the modern digital landscape. However, with the increasing dependence on online platforms, the risk of cyber threats also increases among which phishing continues to be the most prevalent and menacing. Phishing is one of the widespread and hazardous forms of cybercrime breeding in the digital world, tricking individuals into giving their sensitive information such as their passwords and financial information by pretending to be some trusted body safe to enter or provide sensitive data. Although there have been continuous advancements in cybersecurity, Phishing attacks have continued to outgrow the safety mechanisms, employing advanced techniques that exploit loopholes in the current safety mechanisms to curb phishing attacks. Conventional methods, including blacklisting and heuristic-based detection systems, face difficulty to keep track of the changing nature of these threats. These systems depend on known phishing schemes and would not adapt quickly to new ones, hence prone to serious financial and data losses of users and organizations. To answer this growing issue, this system would be developed under PhishNetGuard: a real-time phishing solution.

Keywords- Phishing, LSTM, URL Vectorization.

I. INTRODUCTION

Phishing has been a prevalent variety of cybercrime, tricking individuals into giving their personal and sensitive information to frauds resulting in financial losses. To address these problems, we propose PhishNetGuard, for detection of phishing in real-time driven by the functionalities of artificial intelligence and machine learning. PhishNetGuard monitors suspicious URLs and verifies their structure to detect phishing attempts by a third-party user. The system aims to provide an accurate method of detecting phishing with minimal false positives that protect users from cyber related crimes and ensure they can surf the web without fear. In addition to real-time detection, PhishNetGuard is built to be scalable and adaptable to ensure it follows the trend of continuously evolving phishing attacks. The machine learning models improve their functioning with the discovery of new phishing attempts; thus the system can put forward a more secure and robust solution to emerging threats. The goal of PhishNetGuard is not only to reduce the risk of fraudulent financial activities, stolen identities, and data compromises but also to grow trust and confidence in online activities. Through continuous threat recognition mechanisms, PhishNetGuard aims to create a safer digital environment for all users.

The main purposes of this review are:

1.1 Accurately Identify Phishing Websites: Develop advanced detection systems that have an impact on complex patterns, check suspicious URLs, examine website content, and evaluate structural features to classify legitimate websites and illegitimate ones. This ensures thorough identification while reducing oversights.

1.2 Strengthen Cybersecurity: Implement proactive, multi-layered defense strategies to combat phishing attacks and protect users from serious risks like data breaches.

1.3 Enable Real-Time Detection: Equip users with near-instantaneous phishing by quickly spotting harmful websites with minimal delays. This prevents users from interacting with malicious platforms ensuring smooth and safe browsing.

The upcoming sections are categorized as follows: -
Section 1: Background and Motivation
Section 2: Recent Advances in LSTM-Based Phishing Detection
Section 3: Integration of LSTM and URL Vectorization
Section 4: Evaluation of LSTM-Based Phishing Detection
Section 5: Strengths and Limitations
Section 6: Future Directions
Section 7: Conclusion
Section 8: References

II. BACKGROUND AND MOTIVATION

Table 1: Related Work On Various Models Of Phishing Detection Model

S.NO.	Study Title	Authors	Models Used	Key Features	Year
1	Real-time Phishing detection using deep learning methods by extensions (IJECE)	Dam Minh Linh, Ha Duy Hung, Han Minh Chau, Quang Sy Vu, Thanh-Nam Tran	K-Means, Random Forest , Long Short-Term Memory (LSTM)	Email classification, 160 emails analyzed using technical parameters, structure, and content	2024
2	Improved Detection of Phishing Websites using Machine Learning (IJISAE)	Sumo Sami M Aldaham, Osama Ouda, A.A. Abd El-Aziz	Decision Tree, Random Forest , Support Vector Machine (SVM), ANN	Dataset: PhishTank; preprocessing (normalization), decision tree, data quality improvement	2024
3	A Machine Learning Approach for Phishing Attack Detection	Tarun Choudhary Siddhesh Mhapankar Rohit Bhddha Ashish Kharuk Dr. Rohini Patil.	CNN, Bidirectional LSTM	Combines CNN & LSTM for content-based phishing detection, hyperparameter tuning	2023
4	Detecting Phishing Websites Using Machine Learning Technique	Ashit Kumar Dutta	RNN, LSTM	LSTM for URL detection, analysis of long- term dependencies, classification of websites	2021
5	Research on Website Phishing Detection Based on LSTM RNN	Su Yang	LSTM, RNN	Sequential URL pattern detection, overcoming issues of URL blacklisting	2020

III. METHODOLOGY

This section contains the methodology used in the review paper to discuss the sources for data collection, preprocessing of data, extracting the relevant and important data and model evaluation used in the process of Phishing Detection using LSTM.

3.1 Data Collection

Utilisation of open-sources platforms for data collection such as **PhishTank** and **OpenPhish** for phishing URLs, **AlexRank** for legitimate websites.

Both the datasets were utilized to ensure that there is no class imbalance by maintaining a balanced dataset for the classification task.

3.2 Data Preprocessing

Before performing the classification task, it is required to make the dataset of high quality by carrying out some preprocessing steps like **URL Cleaning** (removal of special character, HTTP/HTTPS prefixes, etc), **Tokenization** (Splitting URLs into meaningful tokens), **Normalization** (Converting all text to lowercase and removing duplicates)

3.3 Feature Extraction Techniques

Feature extraction is carried out on raw URLs to create a meaningful representation, which makes it easier for the LSTM model to process. The techniques include **TF-IDF Encoding** (to extract the statistical importance of words in URLs) **Embedding Representations** using **Word2Vec** (to generate the contextual embedding for words in URLs)

Recent studies have shown that deep learning models, particularly LSTM networks, effectively capture sequential patterns in URLs, improving phishing detection. LSTM models can identify subtle manipulations in URL structure, making them robust against unknown phishing attacks. The model processes the sequential data of URLs to learn phishing patterns, making more accurate predictions about their legitimacy.

3.4 Model Development

To evaluate the performance of LSTM-driven Phishing detection, several models were built and compared

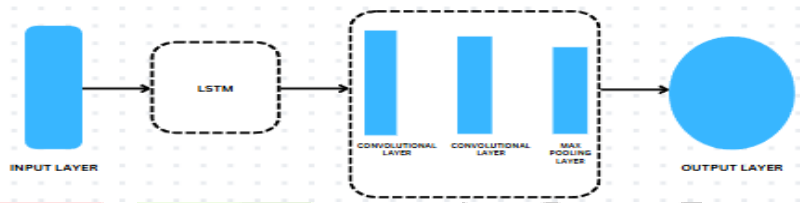
Baseline Models:

3.4.1 Logistic Regression
3.4.2 Decision Trees
3.4.3 Support Vector Machines (SVM)

Deep Learning Models:

3.4.1 LSTM model
3.4.2 Bi-LSTM model
3.4.3 Hybrid CNN-LSTM

Fig 1: Architecture of a typical LSTM model



3.5 Model Training

Data Splitting: The dataset was divided into 80% training, 10% validation, and 10% testing.
Optimization: Adam optimizer was used with an adaptive learning rate scheduler.
Hyperparameter Tuning: Grid Search was applied to optimize learning rates, dropout rates, and layer configurations.

3.6. Evaluation Metrics

The models were evaluated based on standard classification metrics:

3.6.1 **Accuracy** – Measures overall correctness of classification.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

3.6.2 **Precision** – Measures how many detected Phishing URLs were truly Phishing.

$$\text{Precision} = \frac{TP}{TP+FP} \quad (2)$$

3.6.3 **Recall** – Determines how many actual Phishing URLs were detected.

$$\text{Recall} = \frac{TP}{TP+FN} \quad (3)$$

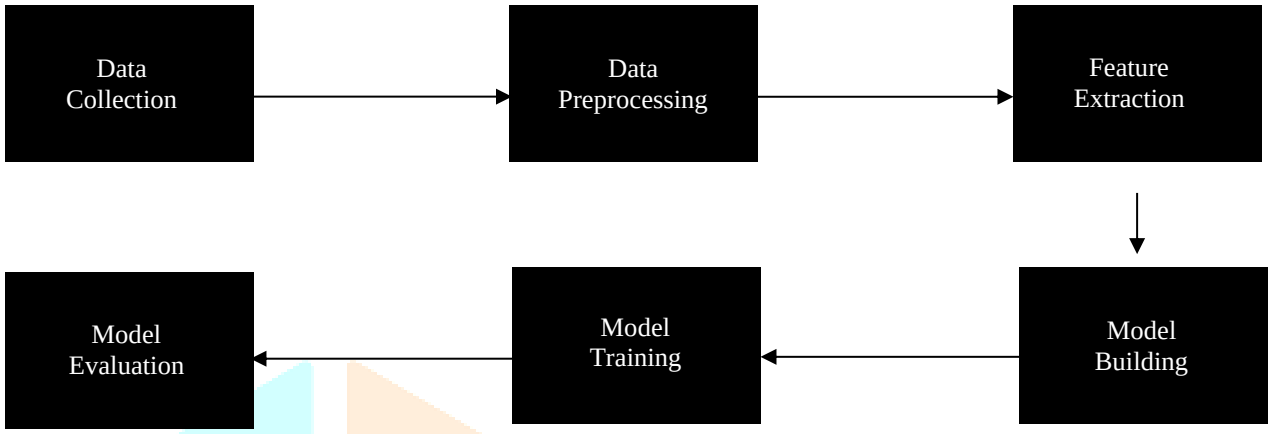
3.6.4 **F1-Score** – Balances precision and recall.

$$\text{F1 Score} = 2 * \left(\frac{\text{Precision} * \text{Recall}}{\text{Precision}+\text{Recall}}\right) \quad (4)$$

Where,

- TP indicates True Positives,
- TN indicates True Negatives,
- FP indicates False Positives,
- FN indicates False Negatives

Fig 2: Workflow of the above methodology used



IV. RESULTS AND DISCUSSION

4.1 Comparison of Performance of the Models

Table 2: Comparison of the existing Phishing detection models for understanding the models in much detail.

Title	Authors	Model/Technique	Key Features	Performance metrics
"Enhancing Phishing Detection: A Novel Hybrid Deep Learning Framework for Cybercrime Forensics"	Faisal S. Alsubaei, Abdulwahab Ali Almazroi, Nasir Ayub.	Hybrid Deep Learning (CNN + LSTM) Approach	Uses CNN and LSTM to capture both spatial and temporal features of phishing data Uses CNN and LSTM to capture both spatial and temporal features of phishing data	Accuracy ~ 98.5%, Precision: 97.8%.
“Website phishing detection using machine learning techniques”	Alazaidah, R.; et al.	Decision Tree Classifier	Utilizes URL-based features and website content analysis to distinguish between legitimate and phishing websites.	Accuracy ~ 95.2%, Recall: 94.5%.
"Phishing URL Detection Using CNN-LSTM and Random Forest Classifier"	Gurung, H.; Nepal, R.; Nepal, S.	CNN-LSTM Hybrid with Random Forest	Combines a Random Forest classifier with CNN and LSTM networks to improve detection.	Accuracy ~ 96.8%, Precision: 96.2%

"AntiPhishStack: LSTM-Based Stacked Generalization Model for Optimized Phishing URL Detection"	Aslam, Saba; et al.	Stacked Generalization with LSTM	Integrates multiple base learners with an LSTM-based meta-learner to enhance phishing URL detection.	Accuracy ~ 97.3%, F1-score: 96.9%
"A Hybrid DNN–LSTM Model for Detecting Phishing URLs"	Ozcan, Alper; et al.	Hybrid DNN and LSTM Model	Analyzes intricate patterns in phishing URLs by combining the advantages of DNNs and LSTMs.	Accuracy ~ 97.1 %, F1-Score: 96.7%

V. CONCLUSION & FUTURE SCOPE

5.1 Strengths and Limitations

LSTM, which stands for Long Short-Term Memory, is a form of RNN that has been highly effective in phishing attack detection. The LSTM model architecture provides features that are best suited for sequential data analysis and the detection of intricate patterns. LSTM networks are especially good at learning temporal relationships in data sequences because of their special memory structure. This enables them to learn long-range dependencies, which is important in the phishing detection process where the sequence of events or interactions can reveal malicious activity. Compared to traditional RNNs, LSTMs assist in retaining information over longer sequences and, therefore, are a suitable option for detecting phishing attempts that a system experiences over time. LSTM models can analyze various types of data, including user behavior patterns, email sequences, and web interactions, to identify phishing attacks. For example, by analyzing the sequence of user clicks or emails, LSTMs can detect anomalous access patterns that can reveal phishing attempts. This feature is valuable because phishing attacks are based on deceptive communications that evolve, requiring dynamic analysis to identify.

LSTM models in phishing detection are optimized using data augmentation, feature extraction, and model-tuning techniques. For example, the Synthetic Minority Over-Sampling Technique (**SMOTE**) can resample training datasets, which are prone to class imbalance between legitimate and phishing instances. Taking advantage of methods like **swarm intelligence algorithms** for feature selection further processes the input to the LSTM model to make them more accurate in phishing variant detection. Nevertheless, continues to address challenges by taking advantage of advances in deep learning and optimization to new phishing methods. LSTMs require large, high-quality datasets for training to generalize well. If the dataset is noisy, biased, or imbalanced, the model's performance can be affected. Phishing content can be generated by attackers with slight modifications to avoid detection attempts (e.g., through homograph attacks, typo squatting, or encoding tricks. Unless trained on sufficient varieties of real-world instances, these LSTMs can miss such slight variations. Real-time detection becomes problematic for LSTMs due to their computational cost of training and inference, as they process an instance one at a time. LSTMs readily overfit, especially when they are complex and with limited training data. They thus provide less benefit to the detection of new or otherwise unseen data. Although LSTMs can model sequential patterns of phishing attacks, they may not consider the whole context or meaning of the attacks, thus more likely to produce false positives and/or false negatives.

5.2 Future Directions

In the upcoming improvements, advancements in phishing detection shall, on the one hand, focus on AI and machine learning technologies that would detect phishing attacks in real-time with high accuracy, countering the attack methods used in any advanced phishing plan. NLP shall greatly assist context-related analysis of messages, emails, and user interactions to strengthen detection of Phishing attempts using linguistic patterns

and suspicious behaviors. URL filtering algorithms will have a stronger foundation to identify advanced phishing techniques: homograph attacks and embedded malicious links. Also, enhanced content inspection techniques will improve phishing protection through the detection of camouflaged and obfuscated content.
Phishing detection will also extend to IoT devices and mobile platforms that are becoming the focus of cybercrime. Lightweight and effective detection algorithms will target resource-limited devices, guaranteeing that all platforms receive appropriate protection. Collaborative threat intelligence networks will be put in place to facilitate real-time phishing data sharing and countering measures among organizations for collective resilience against cyber threats.

Crowdsourcing will be applied towards increases in phishing detection by letting communities find and report phishing pursuits more rapidly, thus actually enforcing the countermeasures. Advocacy will bolster lobbying for more stringent regulation and statutory action against phishing crimes to strengthen the legal framework. Global standards will be created through collaboration among governments and organizations with a view to creating strong and viable preventive measures against phishing that will be worldwide in scope. Cybersecurity systems will put measures in place to counteract quantum computing phishing threats, which may take advantage of obfuscation strategies that are far advanced into the future and bypass most security mechanisms. Ultimately, however, browser extensions and mobile applications will be developed to bring non-technical users real-time alerts about suspicious activities, covering the gap of advanced security systems and user awareness.

5.3 Conclusion

The capture of URLs through vectorization and articulate phishing identification with the aid of Long Short-Term Memory (LSTM) based neural networks has improved rapidly over the years. By analyzing URL structures and patterns, LSTM models can identify minute discrepancies that characterize phishing attacks. This strategy outperforms other heuristic or rule-centred methods that usually have a hard time identifying new phishing techniques due to their accuracy and flexibility. URL vectorization, the process of converting textual URLs into numbers, making it easier for the LSTM models to process this data. By capturing the sequential formation of URLs, contextual information is retained and is not lost. LSTMs are able to learn complex patterns in large datasets which makes them extremely advantageous as phishing methods keep evolving. It has proven to be more effective than traditional heuristic methods which falter in detecting new phishing attacks. However, challenges remain. For one, quality phishing URL datasets are hard to encounter which makes data availability a key issue, as high-quality labeled datasets for phishing URLs are often limited. Additionally, the computational overhead of LSTM models can hinder their deployment in resource-limited environments. Interpretability is also an issue; the ability to explain why a model flags a particular URL is essential for trust and regulatory compliance. Regardless of these challenges, the application of LSTM networks together with URL vectorization may be one of the most promising areas of cybersecurity concern. Future advancements in explainable AI could enhance model transparency, while hybrid LSTM systems will utilize other machine learning techniques. But even more importantly, to be able to detect with immediate response will be necessary to address the more sophisticated phishing threats and strengthen this approach's position for more advanced cybersecurity defenses. approaches may improve efficiency. Moreover, the development of real-time detection capabilities will be pivotal in staying ahead of increasingly agile phishing threats, further solidifying this approach's role in advanced cybersecurity defenses.

VI. REFERENCES

[1] Alkhalil, Zainab, et al. "Phishing attacks: A recent comprehensive study and a new anatomy." Frontiers in Computer Science 3 (2021): 563060.
[2] Alsubaei, Faisal S., Abdulwahab Ali Almazroi, and Nasir Ayub. "Enhancing Phishing detection: A novel hybrid deep learning framework for cybercrime forensics." IEEE Access (2024).

[3] Alazaidah R, Al-Shaikh A, Al-Mousa MR, Khafajah H, Samara G, Alzyoud M, Al-Shanableh N, Almatarneh S. Website Phishing detection using machine learning techniques. Journal of Statistics Applications & Probability. 2024 Jan;13(1):119-29.

[4] Tamal, Maruf A., et al. "Unveiling suspicious Phishing attacks: enhancing detection with an optimal feature vectorization algorithm and supervised machine learning." Frontiers in Computer Science 6 (2024): 1428013.

[5] Aslam, Saba, et al. “AntiPhishStack: LSTM-Based Stacked Generalization Model for Optimized Phishing URL Detection.” Symmetry 16.2 (2024): 248.

[6] Balantrapu, Siva Subrahmanyam. "Evaluating the Effectiveness of Machine Learning in Phishing Detection." International Scientific Journal for Research 5.5 (2023).

[7] Adebowale, Moruf Akin, Khin T. Lwin, and M. Alamgir Hossin. “Intelligent Phishing detection scheme using deep learning algorithms.” Journal of Enterprise Information Management 36.3 (2023): 747-766.

[8] Ozcan, Alper, et al. “A hybrid DNN–LSTM model for detecting Phishing URLs.” Neural Computing and Applications (2023): 1-17.

[9] Alshingiti, Zainab, Rabeah Alaqel, Jalal Al-Muhtadi, Qazi Emad Ul Haq, Kashif Saleem, and Muhammad Hamza Faheem. "A deep learning-based Phishing detection using CNN, LSTM, and LSTM-CNN." Electronics 12, no. 1 (2023): 232.

[10] Raja, A. S., Peerbasha, S., Iqbal, Y. M., Sundarvadivazhagan, B., & Surputheen, M. M. (2023). Structural Analysis of URL For Malicious URL Detection Using Machine Learning. JOURNAL OF ADVANCED APPLIED SCIENTIFIC RESEARCH, 5(4), 28-41.

[11] Pooja, ASSV Lakshmi, and M. Sridhar. "Analysis of Phishing website detection using CNN and bidirectional LSTM." 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA). IEEE, 2020.Le, H., et al. (2023). "URLNet: Leveraging CNN for Phishing Website Detection." Proceedings of the International Workshop on Deep Learning in Cybersecurity.

[12] Jain, A.K., & Gupta, B.B. (2023). "PHISH SAFE: A Decision Tree-Based Phishing Detection System." Proceedings of the Cybersecurity Symposium.

[13] Roy, Sanjiban Sekhar, et al. "Multimodel Phishing URL detection using LSTM, bidirectional LSTM, and GRU models." Future Internet 14.11 (2022): 340.

[14] Dutta, Ashit Kumar. "Detecting Phishing websites using machine learning techniques." PloS one 16.10 (2021): e0258361

[15] Liang Y, Wang Q, Xiong K, Zheng X, Yu Z, Zeng D. Robust detection of malicious URLs with self-paced wide & deep learning. IEEE Transactions on Dependable and Secure Computing. 2021 Oct 2019(2):717-30.

[16] Ariyadasa, Subhash, Subha Fernando, and Shantha Fernando.” Detecting Phishing attacks using a combined model of LSTM and CNN.” Int. J. Adv. Appl. Sci 7.7 (2020):56-67.