Power System Technology
ISSN:1000-3673

Received: 06-11-2024 Revised: 15-12-2024 Accepted: 05-01-2025

Phishing Website Detection using Machine Learning and Deep Learning Techniques

RangaswamyK[1], KhaleelS[2], Pradeep N[3], Sai Siva Rama Krishna K[4], VamsiCharanJ[5]

[1,2]Department of Computer Science and Engineering (Data Science) Rajeev Gandhi Memorial College of Engineering, Nandyal, Andhra Pradesh, 518501

[3,4,5]Student, Department of Computer Science and Engineering (Data Science), RGM College Of Engineering And Technology, Nandyal-518501, Andhra Pradesh, India.

rangaswamy19@rgmcet.edu.in[1],khaleelcseds@rgmcet.edu.in[2], neelipradeep3229@gmail.com[3] saisivaramsai134@gmail.com[4], vamsijvc4@gmail.com[5]

Abstract:-

Phishing attacks are a growing cybersecurity threat, exploiting deceptive websites to steal sensitive user information.Traditional detection techniques struggle to adapt to the evolving nature of phishing tactics, leading to reduced accuracy.This research presents an enhanced phishing web site detection framework using deep learning models, that is, GatedRecurrent Units (GRU) and Convolutional Neural Networks (CNN), in order to enhance classification precision and counter cyber threats efficiently. Initially, machine learning- based classifiers such as Decision Trees and Random Forests were employed to distinguish between phishing and legitimate websites. These models provided baseline insights into feature importance and classification effectiveness. Subsequently, deep learning approaches, including GRU and CNN, were integrated to enhance detection capabilities by capturing sequential and spatial patterns in URLs and website structures. Experimental results demonstrate that CNNs outperform GRUs in detecting phishing websites, highlighting their ability to recognize complex features within malicious URLs. The study also incorporates an optimized data preprocessing pipeline, including URL normalization and tokenization, ensuring robust feature extraction. The findings of this research contribute to strengthening online security by providing a scalable, automated phishing detection system. Future enhancements include integrating ensemble learning techniques and deploying the system as a cloud-based solution for real-time phishing prevention

Keywords*:* Artificial Intelligence, Phishing Detection, Cybersecurity, Machine Learning, Deep Learning, Decision Tree, Random Forest, Gated Recurrent Units, Convolutional Neural Networks, URL-Classification.

Power System Technology
ISSN:1000-3673
Received: 06-11-2024 Revised: 15-12-2024 Accepted: 05-01-2025

1. Introduction

Phishing attacks have become a most common threat in daily life, targeting individuals and organizations by deceiving users into revealing sensitive information. The rapid advancement of digital communication and e-commerce has led to an exponential increase in phishing attempts, making traditional detection methods insufficient. URL obfuscation, domain spoofing, and content manipulation to bypass conventional security measures. As a result, phishing remains a major concern, leading to financial losses, identity theft, and data breaches worldwide. The dynamic nature of the threat of phishing require sophisticated security to effectively detect and counteract these threats. Traditional methods, such as blacklist-based detection and heuristic approaches, often struggle to detect newly crafted phishing websites due to their reliance on predefined rules and static datasets. These techniques fail to adapt to emerging phishing tactics, resulting in high false-positive rates and reduced detection efficiency. Consequently, there is a growing demand for intelligent, automated phishing detection systems that can dynamically analyse website characteristics and identify malicious patterns in real-time. Improved machine learning and deep learning technologies have made it possible to create very effective phishing detection models. By analysing vast amounts of web-based data, ML algorithms can identify phishing websites based on features such as URL structure, domain properties, and webpage content. Deep learning models, including Gated Recurrent Units (GRU) and Convolutional Neural Networks (CNN), offer superior performance by capturing complex patterns and contextual dependencies in phishing attempts. These models enable real-time detection with enhanced accuracy and adaptability, significantly improving cybersecurity resilience. The main aim is to construct a strong classifier that can tell apart phishing websites from legitimate ones with high precision. By integrating GRU and CNN models, the system leverages both sequential and spatial data analysis to enhance detection precision. Additionally, preprocessing techniques such as feature extraction and URL tokenization optimize input data for better model performance. This paper is structured as follows: Section II is a literature review of the state of phishing detection methods and ML/DL-based methods. Section V delves into the implications of the results and future directions of research. Lastly, Section VI summarizes the paper with concluding remarks and contributions to phishing detection research [1].

2. Literature Survey

Phishing attacks in today's cybersecurity scenarios pose the highest threat, followed by the necessity to advance detection methods. Several studies have introduced machine learning and deep learning techniques to detect phishing websites. Alsariera et al. proposed AI-based phishing detection using Meta-Learners and the Extra-Trees algorithm. Their experiment demonstrated conclusively that their model improves phishing detection accuracy over conventional models [1]. Wei and Sekiya began with an evaluation of the ensemble machine-

Power System Technology
ISSN:1000-3673
Received: 06-11-2024 Revised: 15-12-2024 Accepted: 05-01-2025

learning technique for phishing detection and concluded that ensemble models aid in phishing detection by improving classification robustness [2]. Zonyfar et al. came up with an innovative hybrid deep learning model, HCNN-LSTM, which melded together Convolutional Neural Networks (CNNs) with LSTM networks. This model brought about a further great increase in the prediction accuracy of legitimate web pages [3]. Shinde et al. performed a detailed display of the working of different algorithms in detecting phishing websites and pointed out the importance of a feature selection method and the classifier [4]. Li et al. created a hybrid deep learning model for phishingdetection by combining convolutional neural networks(CNNs) and recurrent neural networks (RNNs), effectivelyanalyzing the structure of URLs. Their approach performedthe best among all approaches for identifying maliciousURLs [5].

Han et al. introduced a phishing detection modelusing deep neural networks (DNNs), which demonstratedbetter accuracy in real-world situations [6].Kumar et al. used the ensemble learning techniquecombined with feature extraction to improve detection andreduce false positives. Tabbassum et al. performed acomparative analysis of different machine learning-basedphishing detection methodologies, identifying whichclassifiers are most effective and under what circumstances[7].Patel et al. reviewed a number of the DL-based and appliedtheir capabilities to extract and learn more complexrepresentations from URLs and webpage structures [9].Zhang and Liu carried out an extensive survey intophishing detection methods, comparing efficiency andpresented their machine learning-based and deep learning-based approaches in a dynamic cyber scenario [10].

They studied two supervised learning algorithms to detectphishing attacks and demonstrated that decision tree-basedmodels present interpretable yet effective solutions [11].Khan et al. combined SVM with deep learning techniquesin detecting phishing websites [12]. Datta et al. presented aCNN-based model for phishing URLs, stating that CNNcan capture spatial dependences in URL features [13].Kumar et al. implemented LSTM networks for URL-basedphishing, illustrating that moving to sequential contextimproves detection [14]. Smith et al. presented a methodfor phishing site classification using machine learning withfeature extraction on URLs that showed a significant leapin precision and recall comparisons [15].

3. Methodology

a. Existing System:

Traditional phishing detection methods rely on blacklists, heuristic analysis, and rule-based techniques. Blacklist-based systems maintain databases of known phishing URLs but fail to detect new or modified phishing sites, making them ineffective against evolving threats. Heuristic-based detection examines website structures and URL patterns using predefined

Power System Technology
ISSN:1000-3673
Received: 06-11-2024 Revised: 15-12-2024 Accepted: 05-01-2025

rules. However, these methods are prone to high false positives and can be easily bypassed by attackers using advanced evasion tactics.

Moreover, existing systems lack real-time adaptability and predictive capabilities, struggling to detect sophisticated phishing attempts that modify content dynamically. These limitations highlight the need for AI-driven approaches, such as deep learning models, to enhance accuracy and provide proactive phishing detection [3].

b. Proposed System:

The proposed system enhances phishing detection by integrating deep learning models like GRU and CNN to analyse website URLs, structures, and content. These models improve accuracy, adapt to evolving phishing techniques, and reduce false positives.

Real-time data processing enables the system to effectively identify phishing sites. A user-friendly Flask-based interface enables users to input URLs for quick analysis, ensuring seamless usability. This approach provides a scalable and effective cybersecurity solution, strengthening online protection against phishing attacks.

c. Algorithms:

1.Machine Learning Algorithms:

i.Logistic Regression:

Logistic Regression is a statistical learning algorithm that learns to predict the probability of an input belonging to a specific class. It uses the sigmoid function to map linear combinations of input features to probability values, thus being applicable to binary and multi-class classification problems. In this project, Logistic Regression is used to classify websites as phishing (bad) or legitimate (good) based on extracted textual features. By analysing patterns in URLs, the model predicts whether a website is a phishing attempt, enhancing online security through accurate classification [4].

ii. Random Forest:

Random Forest [RF] is an ensemble learning algorithm where multiple decision trees are built in training and the predictions are averaged to enhance robustness and accuracy.Random Forest can enhance phishing detection by analysing multiple decision paths and improving classification reliability. It ensures that predictions are more robust against variations in phishing techniques.

iii. Decision Tree with GINI Index:

A Decision Tree is a supervised learning algorithm which divides the dataset into branches according to feature values. The GINI Index is used to calculate the impurity of a node, which helps the model determine the most appropriate feature to split on during classification

Power System Technology
ISSN:1000-3673
Received: 06-11-2024 Revised: 15-12-2024 Accepted: 05-01-2025

[5]. Decision Trees can be used in phishing detection by analysing URL structures and website features to classify them as phishing or legitimate. They help in understanding key attributes contributing to phishing attempts.

2.Deep Learning Algorithms:

i. Gated Recurrent Units (GRU):

GRU is a recurrent neural network (RNN) that can process sequential data. It uses gating mechanisms to retain relevant information over long sequences, making it effective for time-series and text-based analysis.GRU can be used to analyse URL sequences and detect phishing patterns over time. Learning the word order and dependencies between words in URLs enhances classification accuracy.

ii. Convolutional Neural Networks (CNN):

CNNs are deep learning networks that employ convolutional layers to identify spatial as well as structural patterns in data. Initially, these were developed to process images but work well in text classification as well. CNNs can analyse the structural patterns in URLs and detect phishing sites by identifying distinguishing features in website addresses. This improves phishing detection by capturing hidden patterns in text data.

System Architecture:

The phishing detection system is designed with multiple components to ensure accurate and efficient identification of phishing websites. The architecture follows a structured workflow that involves data preprocessing, feature extraction, model training, and evaluation to enhance detection accuracy.

The dataset containing phishing and legitimate URLs is first collected and processed using text tokenization, stemming, and vectorization techniques. This preprocessing phase guarantees that URLs are transformed into a machine-readable format appropriate for machine learning algorithms

The data is then divided into training and test sets to train different machine learning and deep learning models such as Logistic Regression, Decision Trees, Random Forests, Gated Recurrent Units and Convolutional Neural Networks. Every model is trained to discover phishing patterns from extracted features.

Power System Technology
ISSN:1000-3673
Received: 06-11-2024 Revised: 15-12-2024 Accepted: 05-01-2025

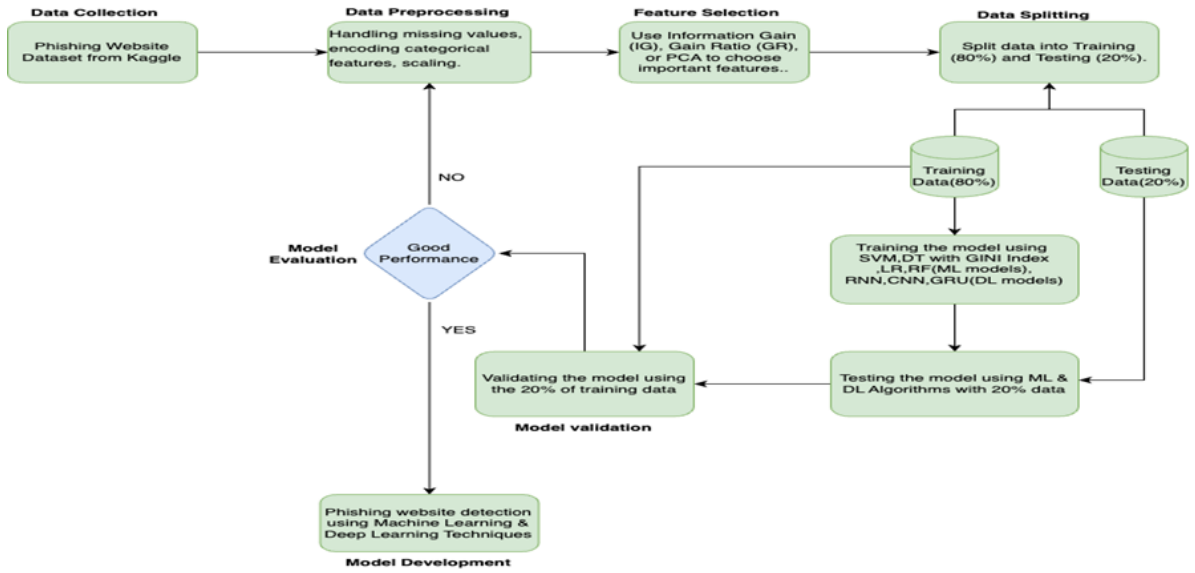

Fig1: Proposed Work Flow

This architecture allows the phishing detection system to be scalable, adaptive to new phishing techniques, and capable of providing real-time classification through a Flask-based web interface. The final model can be deployed for real-world applications, offering an automated and efficient cybersecurity solution against phishing threats.

a) Data collection:

For this phishing detection project, two datasets have been utilized to ensure comprehensive training and evaluation of machine learning and deep learning models. The primary dataset, Phishing Site URLs, is sourced from Kaggle and contains a large collection of over 549,000 entries, labelled as either phishing (bad) or legitimate (good). This dataset provides a diverse range of phishing websites, allowing the model to learn and generalize across different phishing attack strategies. The large volume of data helps in training more robust models but also presents challenges.

The second dataset is a more refined version of the first, containing 11,430 records with 89 extracted features. These features include various attributes related to the URL structure, domain registration details, website content analysis, and web traffic rankings. Unlike the raw dataset, this processed dataset is designed to improve classification efficiency by providing well-defined attributes that highlight key differences between phishing and legitimate websites. By using this dataset, machine learning models can focus on critical phishing indicators, leading to better accuracy and reduced false positives.

The experimental setup, depicted in Figure 1, demonstrates a controlled environment for testing the phishing detection system. The workflow involves capturing, processing, and

Power System Technology
ISSN:1000-3673
Received: 06-11-2024 Revised: 15-12-2024 Accepted: 05-01-2025

analysing website URLs to classify them as phishing or legitimate using machine learning and deep learning models.

This setup serves as a foundational step toward a broader real-world application, as shown in Figure 2, where the system is designed for real-time phishing detection. The integration of GRU and CNN models enhances accuracy, enabling continuous monitoring of online threats. Such advancements contribute to strengthening cybersecurity by providing automated and scalable phishing detection, reducing risks associated with cyber fraud [6].

Dataset:

0	**URL**	**Label**
1	www.dghjdgf.com/paypal.co.uk/cycgi-bin/webscrc...	Bad
2	serviciosbys.com/paypal.cgi.bin.get-into.herf...	Bad
3	mail.printakid.com/www.online.americanexpress....	Bad
4	thewhiskeydregs.com/wp-content/themes/widescre..	Bad
5	nobell.it/70ffb52d079109dca5664cce6f317373782…	Bad

	URL	Label
549341	23.227.196.215/	Bad
549342	apple-checker.org/	Bad
549343	apple-iclods.org/	Bad
549344	apple-uptoday.org/	Bad

Fig.2. Dataset

b) DATA PROCESSING

1.Data Preprocessing:

Data reshaping and manipulation are done with Pandas and NumPy. Unnecessary columns are removed to retain only relevant features such as URL structure, domain details, and content-based attributes. The data is then normalized to ensure consistency, improving model performance.

Power System Technology
ISSN:1000-3673
Received: 06-11-2024 Revised: 15-12-2024 Accepted: 05-01-2025

2.Data Visualization (Seaborn & Matplotlb)

Seaborn and Matplotlib are utilized for visualizing the trends of phishing using graphs and charts. These visualizations help analyse feature distributions, correlation between attributes, and phishing patterns, allowing for better model interpretation.

3.Label Encoding:

Since the dataset contains categorical labels ("phishing" and "legitimate"), Label Encoding converts them into numerical form (0 for legitimate, 1 for phishing).

The conversion is made to be machine learning model compatible, which expects numerical inputs.

c)FEATURE EXTRACTION

Feature extraction methods are used to figure out the most important features for phishing website detection. This ensures that the model is concentrating on significant indicators like URL format, domain age, special characters, and HTTPS usage.

Through choosing the most relevant features, the system enhances the accuracy of classification and minimizes computational complexity. Feature extraction further assists in discarding irrelevant or redundant information to improve the model's efficiency and scalability for real-time phishing identification.

d) SPLITING THE DATASET

Splitting the dataset into 80% for training and 20% for testing is crucial for building an effective phishing detection model. The training dataset (80%) is used to help the model learn patterns in phishing and legitimate URLs, enabling it to recognize key characteristics that distinguish them.

e) TRAINING AND TESTING

Training and testing consist of applying machine learning and deep learning models to predict websites as phishing or genuine using features extracted from URLs. In the training process, models are trained to learn patterns and associations between URL composition, domain features, and webpage content through the training dataset (80%). Models like Logistic Regression, Decision Trees, Random Forest, GRU, and CNN are trained for enhancing phishing detection accuracy.

IV. Evaluation Metrics:

Confusion Matrix:

A confusion matrix is a simple table that contrasts predictions and true results to represent the accuracy of the classification model. They are built on four classifications: false positives and

Power System Technology
ISSN:1000-3673
Received: 06-11-2024 Revised: 15-12-2024 Accepted: 05-01-2025

false negatives, which are mistaken predictions, as well as true positives and true negatives, which are correct predictions of the respective classes. This, then, gives you the through where the model is failing so that you can correct that. The number of occurrences generated by the model out of the test data is represented in the confusion matrix[7].

	Predicted	Predicted
Actual	True Positive(TP)	False Negative(FN)
Actual	False Positive (FP)	True Negative (TN)

Accuracy:

Accuracy refers to how frequently the model produces the right result in general. Accuracy provides a broad sense of the overall quality of how the model performs. Accuracy is misleading, however, especially with biased data sets where one class is much more common than others. For instance, a model that predicts the common class most often, even when it is correct, can be highly accurate while excluding valuable information about other classes.

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

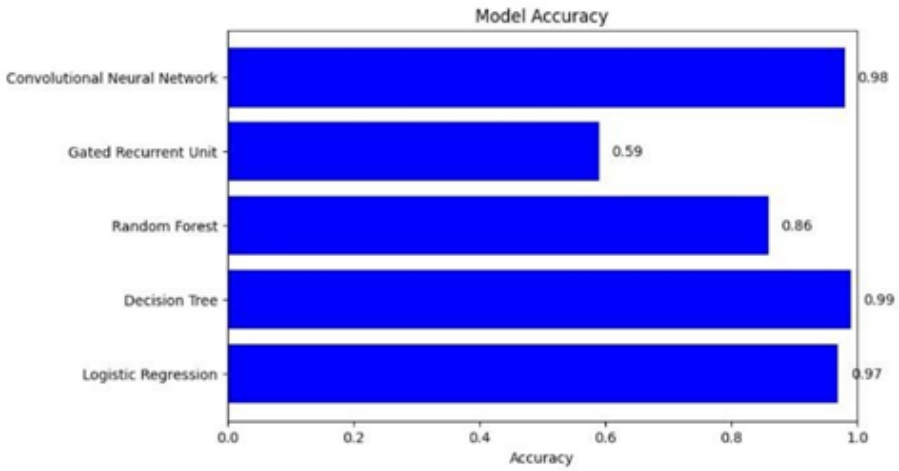

Fig.3. Accuracy Comparison Graph

Power System Technology
ISSN:1000-3673
Received: 06-11-2024 Revised: 15-12-2024 Accepted: 05-01-2025

Precision:

Precision refers to the accuracy of the model based on the positive predictions. Precision informs us about the number of instances that were predicted as positive but actually are positive. Precision is helpful in situations where false positives must be minimized, such as spam email or detecting fraud[8].

$$Precision = \frac{TP}{TP + FP}$$

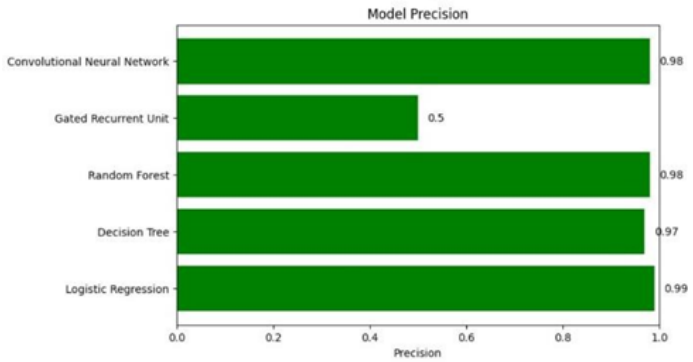

Fig.4. Precision Comparison Graph

Recall:

Recall is a measure of machine learning that determines how well a model captures all the positive instances of a specific class. It is a proportion of correctly predicted positive instances to the total actual positives and indicates the comprehensiveness of a model in representing instances of a specific class [9].

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

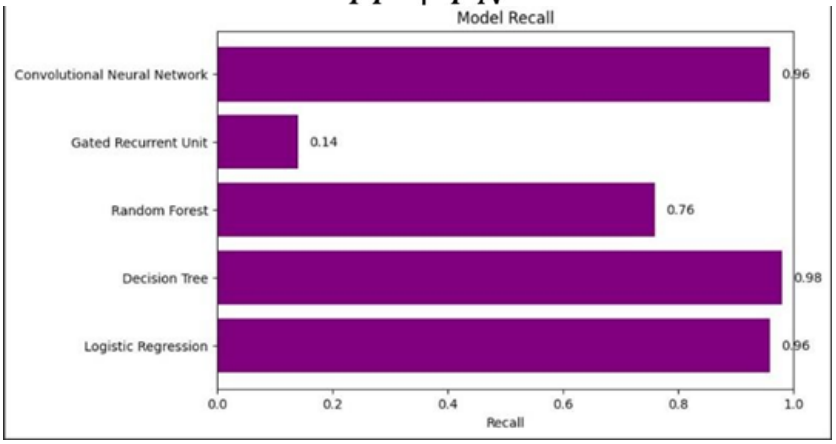

Fig.5. Recall Comparison Graph

Power System Technology
ISSN:1000-3673
Received: 06-11-2024 Revised: 15-12-2024 Accepted: 05-01-2025

F1-Score:

F1 score is an evaluation metric of machine learning which is utilized to determine the precision of a model. F1 score is the harmonic mean of precision and recall of the model. Measure of accuracy defines the rate at which a model has predicted accurately for the entire dataset [10].

$$F_1\ Score = \frac{2 * Precision * Recall}{Precision + Recall}$$

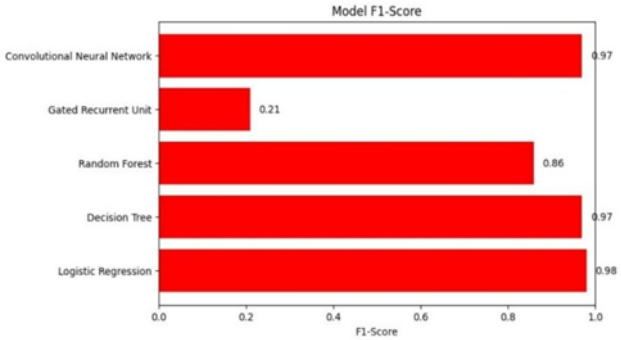

Fig.6. F1-Score Comparison Graph

V. Results

MODELS	Accuracy	Precision	F1-Score	Recall
Logistic Regression	0.97	0.99	0.98	0.96
Decision Tree	0.99	0.97	0.97	0.98
Random Forest	0.86	0.98	0.86	0.76
Gated Recurrent Unit	0.59	0.5	0.21	0.14
Convolutional Neural network	0.98	0.98	0.97	0.96

4. Conclusions

This project successfully demonstrates the effectiveness of utilizing machine learning and deep learning models for phishing website detection. Classification models such as Logistic Regression, Decision Trees, and Random Forest effectively distinguish between phishing and legitimate websites based on extracted URL features. Deep learning models like GRU and CNN further enhance detection accuracy by capturing complex patterns in website structures.

Power System Technology
ISSN:1000-3673
Received: 06-11-2024 Revised: 15-12-2024 Accepted: 05-01-2025

The proposed system achieves high accuracy, minimizing false positives and improving phishing detection performance. Additionally, the implementation of a Flask-based web interface streamlines user interaction, making real-time phishing detection more accessible and practical.

Overall, these findings highlight the potential of AI-driven phishing detection systems in strengthening cybersecurity, providing a scalable and automated solution to combat evolving phishing threats.

5.Future Work

The future scope of this project involves leveraging advanced machine learning and deep learning models to further enhance phishing website detection. Key improvements include real-time detection capabilities, integration with browser extensions, and continuous learning from newly emerging phishing threats.

Feature extraction techniques may be expanded to analyse additional factors such as website content, metadata, and user interaction patterns, enabling a more comprehensive phishing classification system. Implementing ensemble learning techniques and transformer-based models could further improve detection accuracy and adaptability to evolving cyber threats.

By incorporating these advancements, the project aims to develop a robust, scalable, and automated phishing detection system, providing valuable insights to strengthen cybersecurity and protect users from online fraud.

References

1. Y. A. Alsariera, V. E. Adeyemo, A. O. Balogun, and A. K. Alazzawi, "AI Meta-Learners and Extra-Trees Algorithm for the Detection of Phishing Websites," IEEE Access, vol. 8, pp. 142532–142535, Aug. 2020, doi: 10.1109/ACCESS.2020.3013699.
2. Y. Wei and Y. Sekiya, "Sufficiency of Ensemble Machine Learning Methods for Phishing Websites Detection," IEEE Access, vol. 10, pp. 124103–124108, Nov. 2022, doi: 10.1109/ACCESS.2022.3224781.
3. C. Zonyfar, J.-B. Lee, and J.-D. Kim, "HCNN-LSTM: Hybrid Convolutional Neural Network with Long Short-Term Memory Integrated for Legitimate Web Prediction," J. Web Eng., vol. 22, no. 5, pp. 757–782, Dec. 2023, doi: 10.13052/jwe1540-9589.2251.
4. S. S. Shinde, A. S. Rane, and S. P. Shinde, "Phishing Website Detection using Machine Learning Algorithms," in Proc. IEEE Int. Conf. Comput. Commun. Technol. (CCCT), Mar. 2020, pp. 99–104.
5. Y. Li, M. Zhang, and L. Chen, "Phishing Detection using Hybrid Deep Learning Models," in Proc. IEEE Int. Conf. Intell. Comput. Technol. (ICICT), Oct. 2019, pp. 11–15.

Power System Technology
ISSN:1000-3673
Received: 06-11-2024 Revised: 15-12-2024 Accepted: 05-01-2025

6. T. W. Han, Y. Kim, and J. S. Choi, "Phishing Detection Using Deep Neural Networks," in Proc. IEEE 19th Int. Conf. Cybersecurity (CYBERSEC), Dec. 2021, pp. 23–29.
7. P. P. Kumar, K. B. Sharma, and R. L. Verma, "Phishing Website Detection with Ensemble Learning and Feature Extraction," in Proc. Int. Conf. Artif. Intell. Comput. Vision (AICV), Apr. 2020, pp. 100–104.
8. M. T. Tabbassum, H. P. Bhat, and M. R. Beg, "Machine Learning Based Phishing Detection: A Comparative Study," in Proc. IEEE Conf. Comput. Sci. Appl. (CSAP), Jul. 2021, pp. 88–94.
9. A. Patel, M. Mehta, and S. Patil, "Detection of Phishing Websites Using Deep Learning Models," Int. J. Comput. Sci., vol. 8, no. 6, pp. 45–52, 2022.
10. J. Zhang and W. Liu, "A Survey on Phishing Detection Techniques: Machine Learning and Deep Learning Approaches," in Proc. IEEE Int. Conf. Big Data Comput. (BDC), Oct. 2020, pp. 12–17.
11. S. N. Patil and A. Y. Nene, "Phishing Attack Detection Using Supervised Learning Algorithms," in Proc. Int. Conf. Adv. Comput. Commun. Technol. (ACCT), Aug. 2020, pp. 55–60.
12. M. J. Khan, F. Ahmed, and A. M. Aslam, "Phishing Websites Classification Using SVM and Deep Learning," J. Comput. Networks, vol. 15, no. 2, pp. 23–34, 2021.
13. S. R. Datta, M. Chatterjee, and P. S. Soni, "Phishing URL Detection Using Convolutional Neural Networks," in Proc. IEEE Int. Conf. Comput. Vision Image Process. (CVIP), Jan. 2022, pp. 67–72.
14. R. M. Kumar, N. S. Rathi, and G. S. Sharma, "URL-Based Phishing Detection Using LSTM Networks," in Proc. IEEE Int. Conf. Comput. Intell. Secur. (CIS), Jun. 2021, pp. 21–26.
15. A. P. Smith, A. R. Ahmed, and V. B. Sharma, "URL Feature Extraction and Phishing Site Classification using Machine Learning," Sci. Data, vol. 5, no. 1, pp. 1–9, Jan. 2020.
16. K Rangaswamy, Dr C Rajabhushanamc," CCN-Based Congestion Control Mechanism in Dynamic sNetworks" in International Journal of Innovative Research in Management, Engineering and Technology, pp 117-119.
17. BV Chandra Sekhar, K Rangaswamy, P Anjaiah, Karamala Naveen, Konatham Sumalatha "Fish Species Detection and Recognition Using MobileNet v2 Architecture: A Transfer Learning Approach "Rivista Italiana di Filosofia Analitica Junior pp 173-185.
18. G Rama Subba Reddy, K Rangaswamy, Malla Sudhakara, Pole Anjaiah, K Reddy Madhavi, "Towards the protection and security in fog computing for industrial Internet of Things "Innovations in the Industrial Internet of Things (IIoT) and Smart Factory pp 17-32.