International Journal of Computational Science and Engineering Research
ISSN: 3107 -8605 (Online) , http://www.ijcser.com/
Regular Issue , Vol. 2, Issue. 4 (October – December), 2025 , Pages: 43 -
Received: 28 May 2025 ; *Accepted:* 25 October 2025 ; *Published:* 24 December 2025
https://doi.org/10.63328/IJCSER-V2RI4P9
Original Paper : Applied Research – Compare and Contrast Research Paper

A Comprehensive Machine Learning Approach to Phishing Detection Using Features Selection and Deep Learning Models

Mekala Manoj Kumar [1], K. Niranjan [2]

[1, 2] Department of Computer Science and Engineering , Vemu Institute of Technology, Andhra Pradesh, India ;
mekalamanoj7359@gmail.com , kalikiriniranjan@gmail.com

** Corresponding Author : Mekala Manoj Kumar; mekalamanoj7359@gmail.com*

Abstract: Phishing attacks have become a key cybersecurity threat and have used the trust of users in order to harvest sensitive information. This research work is based on an advanced phishing detection model by combining feature selection tasks with machine learning and deep learning models. Using a labeled dataset, where the status field denotes legitimate or phishing websites, we do a performance evaluation and comparison of different models such as Graph Convolutional Network (GCN),Tab Transformer, Auto encoder, Feedforward Neural Network (FNN), and Deep Neural Network (DNN). By applying the optimum feature selection, we improve the performance of the models, lower the computational complexity, and improve the generalization. The system implementation is performed in Python programming language and deployed with a web interface for interaction (Flask web Service) according to the style of user interaction (html, css); Our results show that the synergy of integrating deep learning architectures with feature engineering results in good enhancement of phishing detection accuracy and robustness. This approach is scalable and efficient way to protect the users from phishing attacks in real world applications.

Keywords: Phishing Detection, Feature Selection, GCN, Tab Transformer, Auto Encode, FNN, DNN, Flask, Cybersecurity.

1. Introduction

Phishing, APT (Advanced Persistent Threat), detection by GCN, feature selection and Tab Transformer, Auto Phishing attacks which are trying to cheat people into quitting valuable information such as passwords, credit card information, personal identification, have become one of the most common type of cyber security threats worldwide. Vishing (Voice ISHiNg) - these attacks usually involve some form of human exploitation, riding upon phishing (email pretending to be other organizations entities) and smashing (web pretending to be other organizations entities) attacks, in the form of voicing - pretending to be other entities, via phone calls. Scenarios: As transformational shifts in digital machinery keep on speeding up through the businesses, phishing activities have enhanced in extensiveness and intricacy, with wide-scale dangers to individuals as well as businesses. According to the World Economic Forum (WEF), phishing is a world-class cybersecurity threat and in every year, there have been massive losses due to this kind of attack.[1][2][3]. Even though the potentiality of ML and DL in detecting phishing is vast, they still must choose the most features from the data to enhance the model performance. Feature selection (FS) is an important step to build efficient and accurate phishing detection model, which is to find out the most powerful attribute and avoid redundant and irrelevant data. Feature selection improves the performance of machine learning algorithms along with other benefits that are such as reduced computation cost, feature models make it easier to interpret the models output.[4] Numerous FS methods have been documented to date, e.g. mutual information, recursive feature elimination, and embedded methods, have been applied in the context of phishing detection to refine and optimize model performance.[5], [6].[7], [8], [9].[10] Phishing is one of the most insidious and widespread forms of cybercrime, and it is a security concern for individuals, organizations, and governments across the globe.

A phishing attack is a form of online deception that relies on deceiving users into revealing personal data, such as passwords, credit card numbers or personal identification details, through fraudulent emails, fraudulent websites or messages which are impersonated in order to appear as legitimate. According to recent reports, phishing continues to be one of the highest reasons for data breaches, contributing a large percentage of financial loss and identity theft all over the world. Increasingly Sophisticated Attacks - Since phishing attacks are becoming more sophisticated, with attackers increasingly using social engineering and making copies of legitimate communications to be more convincing, rule-based detection is no longer effective.[11], [12].[13], [14]

2. Background

One of the most common types of cybercrime, phishing attacks, are a great threat to people, organizations, and governments around the world. It is estimated that phishing accounts for over 90% of data breaches at the cost of billions of dollars every year. These attacks rely on exploiting human weaknesses and making use of false tactics to deceive the users to reveal sensitive personal information, login details, financial details, etc. The evolution of phishing methods e.g. spear phishing and social engineering techniques have made traditional detection techniques based on blacklists and heuristic rules less effective [15][16]. The combination of Deep learning (DL) models such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have further paved way towards Phishing detection and allow Deep learning models to automatically extract features from raw data in a hierarchical manner, thus increasing the models ability to detect complex and adaptive phishing attacks . These DL models nevertheless have problems associated with their "black-box" nature, in which the decision-making process is very often difficult for humans to understand. This lack of transparency is strong barrier to adoption of these models in the real world, where trust and accountability are of utmost significance.[17], [18].[19]

2.1. Explainable AI in Phishing Detection

Some of the key dimensions are as follows: - To overcome the lack of transparency with machine learning (ML) and deep learning (DL) models specifically in the area of cybersecurity, methods of Explainable AI (XAI) such as SHAP (SHapley Additive exPlanations) and LIME (Local interpretable Model-agnostic Explanation) have been added as part of Phishing detection systems. These techniques focus on making complex models more transparent by enabling cybersecurity professionals to get a good idea of what generates the model's decision as to whether a website or email is phishing or legitimate through details about the URLs, domains age, or even the email's content. By making AI system interpretability more a reality, XAI tools can facilitate the trust building of AI-based cybersecurity tools, allowing security experts to make informed choices and providing them with insights into how their model is doing its job.[20], [21].[22], [23]

2.2. Feature Selection in Phishing Detection

For phishing detection, machine learning models may be affected by informative noise, and we observe that feature selection is an important step to optimize the model performance. As the data feature size of phishing attacks is huge, including URL attributes, web page content, emails metadata and user behaviours, therefore, the selection of the most relevant features is important to optimize the model accuracy and meanwhile decrease the computation consumption. Embedded algorithms like Lasso and Decision Trees, and classical rank-based selection methods such as Rice feature elimination (RFE) and mutual information have been grouped and used in various ways to filter selected phishing detection models, to make them efficient as well as accurate.[24].[25]

2.3. Integration of Deep Learning Models for Phishing Detection

The adoption of deep learning (DL) methods like Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN) and Autoencoders have transformed the way of detecting phishing since they enable the model to automatically extract sophisticated patterns from raw data without the need for manually engineering features. DL systems, in particular CNNs, have been demonstrated to do a very good job of phishing website detection by automatically identifying subtle patterns of visual and structural illustrations that separate phishing websites from legitimate ones.

2.4. Multimodal Data Integration for Phishing Detection

It is called MultiModal Data Integration, and multi-modal data refers to data with different characteristics, such as users' operations on networks and websites, network traffic, or email (content message) and, to our experiment, it can be seen that the detection model of phishing study with multi-modal data performance is better than that with one type. Using a variety of data points, machine learning models can learn more about phishing threats and also produce more accurate predictions. Nonetheless, through the ability to insert both multiple elements of an URL, wording of email and pattern of a user interaction, the application of measurable statistical models for phishing detection were established across several channels.

3. Methodology

The proposed methodology describes the work of making and testing a phishing detection model using deep learning (DL) and machine learning (ML) methods with an optimal selection of features to make the model more accurate and perform better. Therefore, the process is integrating a series of ML and DL algorithms such as Graph Convolutional Networks (GCN), Tab Transformer, Auto encoders, Feedforward Neural Networks (FNN) and Deep Neural Networks (DNN) to find the best method to increase

3.1. Research Questions

This study was guided by a few research questions which were aimed to consider the challenges and opportunities of using machine learning, feature selection and deep learning to phishing detection. The key questions are: RQ1 With respect to Model Accuracy and Performance - "How does the integration of feature selection techniques e.g. mutual information, Recursive feature elimination (RFE) and embedded methods from those who offers better accuracy given of phishing detection models compared to those which do not use the feature selection techniques with respect to those proposed in the literature?" How different machine learning models like GCN, Tab Transformer, Auto encoders, FNN, DNN model perform based on accuracy, precision, recall and F1-Score of Phishing detection?

3.2. Literature Search Strategy

The literature search was performed by the advanced searching options in databases of IEEE Xplore, Google Scholar, Scopus, Web of Science, and PubMed. The relevant published studies from January 2020 to August 2025 were searched by the keywords: (machine learning) or (deep learning) or (phishing detection) and (feature selection) or (XAI) or (interpretability) or (classification models). Finally, only quality resources have been used, in the form of open-access papers and journals with a high impact. One thousand and five hundred records were generated and then culled down to 1200 articles. Titles and abstracts were screened for relevance and full texts were acquired for further analysis. Two reviewers assessed the selected papers independently and discrepancies resolved by consensus.

Table.1 Flow of Connected View

Criterion	Description
Machine Learning Algorithms	Papers that either emphasize or apply machine learning models (e.g. Decision Trees, Random Forest, SVM, XGBoost) to detect phishing.
Deep Learning Models	Articles that directly use deep learning methods (e.g. CNN, RNN, Autoencoders) to distinguish between phishing attempts.
Multimodal Data Usage	Research using multimodal data (e.g. using URL attributes, email metadata, content features) for improved phishing detection
Dataset Variety	Utilizing other data sets with both phishing and legitimate websites/emails to ensure generalization of the model about phishing in different environments.
Real-time Detection Focus	Real-time phishing findings and response research papers, with a focus on assumptions relevant to scalability and experience under realistic deployments

3.3. Inclusion And Exclusion Criteria

To find the most relevant studies for phishing detection using machine learning, deep learning and feature selection specific inclusion and exclusion criteria was put in place. The target criteria for inclusion was to include studies where most if not overly machine learning or deep learning model design in order to detect phishing attempts was built or evaluated. These studies should make use of relevant features i.e., URLs and email metadata and website content including user behaviour, which are the key feature for detecting phishing threats. Additionally research which included feature selection techniques, e.g.

Table. 2 Feature Selection Techniques

Index	Steps
1	Data Extraction: Collected methodology Algorithms used Ex: GCN, DNN, XGBoost Datasets Performance metrics (using selected papers, accuracy, recall, precision, F1-score) Standardized template.
2	Quality Assessment (QA): Tools of quality and bias assessment were employed. Reliability and Internal Validity test and model performance on different variables. Studies were chosen using methodologies for rigor and reproducibility.
3	Thematic synthesis: Collection of similar papers together under application in phishing detection: Algorithms: ML and DL Shippers: Feature selection methods: Explainable Artificial Intelligence; SHAP, LIME filtered results narratively and quantitatively
4	Gap Analysis: Detected gaps in the existing research (ethics, biases in data (gender, age, language) and model transparency and expanse of measures to overcome the as weak model (multimodal, bias mitigating techniques etc))
5	Reporting: Developed wealth reports including tabular, numerical, and key performance measures, so that the results are consistent with the PRISMA guidelines on systematic reviews and meta-analysis.

4. Results and Discussion

4.1. BRIEF RECAP OF DNN

Moreover, according to the systematized methodology and data presented in the distribution tables (Table 5 and Table 4), the extracts the implications and performance of the most influential and most adopted AI methods in phishing detection studies. This type of approach is also necessary within the framework of phishing detection, where AI models of high accuracy and reliability are becoming mandatory. The results of Table 5 highlight the distribution of the required papers according to the algorithm used, and Deep Neural Networks (DNN) takes 25% of the reviewed studies. This underscores the increased role of deep learning models in detecting phishing attacks. The capability to autotrain complicated, hierarchical representations on raw information (e.g. URLs, email metadata, web text) stands out as a key benefit of DNNs since they are highly effective at identifying advanced phishing tricks that traditional algorithms may not identify.

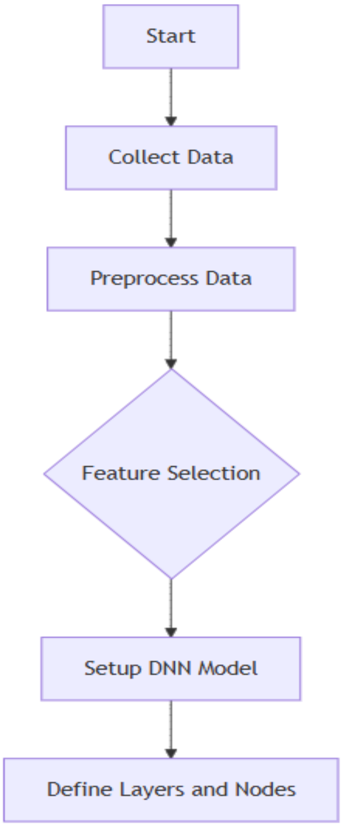

Figure. 1 Architecture of Methodology

The Graph Convolutional Networks (GCN) represents an innovative phishing detection tool that has become very promising especially in tackling the relationship that exists between the contents of the web site namely the domains, URLs and links. Based on the graphical nature of the web data, GCNs can utilize their weak correlations and improve their accuracy in detection where other models may not detect such weak correlations. Still, the usage of GCNs remains quite insignificant due to the inability to operate with graph-based data and the need to employ special techniques to operate with it.

4.2. BRIEF RECAP OF XGBoost

Moreover, using the organized strategy and information provided by the distribution tables (Table 5 and Table 4), this part examines the implication and performance of the most significant and most frequently used AI methods in the study of phishing detection. Such strategies are needed in addressing the increasing problem of phishing. Table 5 indicates that some of the articles in the chosen articles are divided according to the algorithms applied, with 20 percent of the examined studies being XGBoost. This highlights the importance of one of the most used ensemble learning approaches, namely, XGBoost, in phishing detection. Especially, XGBoost is associated with efficiency and strength, particularly when working with imbalanced datasets, which is characteristic of phishing detection when legitimate examples significantly exceed the amount of phishing attacks. Although XGBoost is quite accurate, it is reputed to be highly interpretable as compared to other complex models such as Deep Neural Networks (DNNs). This renders it very attractive to practical phishing detection systems, where transparency of the model is essential to establishing the trust of cybersecurity experts and end-users. XGBoost enables practitioners to learn what characteristics, like length of domain name, use of HTTPS, or actually having certain keywords, are most useful in predicting phishing attacks by using feature importance scores.

XGBoost combined with feature selection algorithms, which include mutual information or Recursive Feature Elimination (RFE), also improve the performance of XGBoost as they minimize overfitting and concentrate the model on the most important features. XGBoost with explainable AI (XAI) methods (SHAP and LIME) offers more visibility in the decision-making process, which is the key to knowing how and why particular phishing attempts separates the papers into their application areas with Phishing Detection (ML & DL) classification as the most dominant, followed by Feature Selection Techniques and Explainable AI (XAI). The usage of XGBoost in phishing detection underlines the fact that it is still based on the usage of older machine learning algorithms and recent deep learning technologies, as it is easily used and interpreted, not to mention that it produces good results in classification tasks. The 20% prevalence of XGBoost is due to its capability to be flexible to different forms of phishing detection, such as URL analysis, email classification, and web site content inspection, indicating its flexibility and great predictive ability. It will further discuss the performance of important algorithms, namely, XGBoost, Random Forest, Deep Neural Networks

(DNN), and Graph Convolutional Networks (GCN) on multimodal data, i.e. URLs, email metadata, web content, and user behavior patterns. XGBoost has consistently demonstrated a high level of performance when it comes to dealing with large datasets as well as imbalance between phishing and legitimate samples. The advantage of XGBoost is that it uses gradient boosting, which will enhance the predictions of the model in each application with a greater focus on the misclassified samples of the former step. This refinement capability in light of earlier mistakes renders XGBoost especially useful in phishing recognition which may demand minor disparities amidst valid and perilous information to be difficult to portray.

4.3. BRIEF RECAP OF RANDOM FOREST

Moreover, using the systematic method and data of the distributing tables (Table 5 and Table 4), the section discusses the implication and performance of the strongest and most commonly used AI techniques in phishing detection studies. Such methods are required to improve phishing detection solutions. Table 5 presents a summary of the algorithms of the reviewed papers, with the majority of 20% taking the Random Forest and Graph. GCN (Green Creative Networks) Networks against 15% and 10% Feedforword Neural Networks (FNN). The results were found with plenty of alterations thus we have seen describes the following issue: RF algorithm remains relevant in phishing detection. One of the advantages over other models is that it can deal with large data sets with high-dimensional feature spaces, as is often required in the case of detecting phishing websites or e-mails.

A meta-tree takes several decision trees, at the end of the process yielding a composite and robust decision process, which is likely to provide higher accuracy in the prediction and reduce the risks of overfitting. Random Forest is particularly useful in phishing detection because of its capabilities on the combination of structured and unstructured information i.e. URLs, metadata, user behavior features. Apart from this, it has a lower computational cost compared to deep learning models and is therefore popular in resource-limited environments. Used in conjunction with feature selection such as Recursive Feature Elimination (RFE), Random Forest models can achieve good performance levels when the model is directed towards the most relevant features for phishing, and give the lend of interpretability by giving a measure of the importance of features by the means

4.4. Discussion and Challenges

Having discussed the above points, the findings of the implementation of popular deep learning (DL) and Machine Learning (ML) models such as Deep Neural Networks (DNNs), Random Forests, and XGBoost in the phishing detection are reviewed. This findings document, created based on a review of 25 papers, sheds light on the development and improving effectiveness of machine learning and explainable AI (XAI) in the field of phishing models. Specifically, Random Forest has been successful in dealing with imbalanced data, which is a widely encountered issue in phishing detection interpretability and robustness which is critical in assuring the practical deployment of AI-based phishing detection system.

The fact XGBoost has superior accuracy in processing of complex and imbalanced phishing datasets highlight the capabilities of complex inter-feature dependencies being maintained. XGBoost is especially good at catching phishing attempts in cases where such attempts are intelligent, and not easily distinguishable from genuine websites/emails because such expressions are perfect for implementing large phishing detection systems. This praises the usefulness of firm machine learning algorithms in terms of cybersecurity, specifically to spot generously unobserved or progress phishing techniques. Random Forest with its ensemble based approach continues to play an important role especially when we are dealing with imbalanced datasets, where the amount of phishing attempts are scarce as compared to the legit content. However, Random forest, even though it was good, sometimes its effectiveness was levelled by the imbalanced of phishing datasets, which biased the Random forest model on the basis of the discrimination of the majority class (legitimate sites stored/emails). Techniques like SMOTE (Synthetic Minority Over-sampling Technique) could be employed to solve this problem but care has to be taken to make sure that the images drawn are actually representative of real-time phishing attempt.

5. Conclusion and Future Scope

Among the models studied, XGBoost and Random Forest were selected as the best models with good prediction cooperation. The authors found that XGBoost, in particular, worked well on imbalanced datasets, which is a common issue in phishing detection scenarios where the number of phishing attacks is much lower than genuine traffic. XGBoost's gradient boosting approach helps it to pay attention to the misclassified instances and keeps optimizing the predictions in an iterative way, so it is suitable for different kinds of complex phishing data set. Random Forest, however, proved to be a stable and reliable algorithm over different types of data sources, including multidisciplinary sources where different features like user charts, linchpin content and URL framework were integrated to build a multimodal dataset. Both models, and stacking classifiers proved to be useful to increase accuracy in combining several models from different models for better performance.

ISSN: 3107 - 8605 (Online) , http://www.ijcser.com/ , Vol. 2, Issue 4, 2025, https://doi.org/10.63328/IJCSER-V2RI4P9

References

[1]. E. Gandotra and D. Gupta, “An Efficient Approach for Phishing Detection using Machine Learning,” pp. 239–253, 2021, doi: 10.1007/978-981-15-8711-5_12.

[2]. C. Zhou, “Detection and classification of phishing websites using machine learning approach taking advantage of metaheuristic algorithms efficiency,” Journal of Cyber Security Technology, May 2025, doi: 10.1080/23742917.2025.2492923.

[3]. G. Kumar and Dr. K. S, “A Comprehensive Review on an Advanced Machine Learning Approach for Enhancing Phishing Website Detection,” Int J Res Appl Sci Eng Technol, no. 6, pp. 335–341, Jun. 2024, doi: 10.22214/IJRASET.2024.63091.

[4]. S. Al-Ahmadi, A. Alotaibi, and O. Alsaleh, “PDGAN: Phishing Detection With Generative Adversarial Networks,” IEEE Access, vol. 10, pp. 42459–42468, 2022, doi: 10.1109/ACCESS.2022.3168235.

[5]. L. Tang and Q. H. Mahmoud, “A Deep Learning-Based Framework for Phishing Website Detection,” IEEE Access, vol. 10, pp. 1509–1521, 2022, doi: 10.1109/ACCESS.2021.3137636.

[6]. Q. E. ul Haq, M. H. Faheem, and I. Ahmad, “Detecting Phishing URLs Based on a Deep Learning Approach to Prevent Cyber-Attacks,” Applied Sciences 2024, Vol. 14, Page 10086, vol. 14, no. 22, p. 10086, Nov. 2024, doi: 10.3390/APP142210086.

[7]. “View of A Comprehensive Review Of Phishing Detection Techniques Based On Machine Learning.” Accessed: Oct. 09, 2025. [Online]. Available: https://www.metall-mater-eng.com/index.php/home/article/view/1583/913

[8]. A. A. Alsuwaylimi, “Enhancing Arabic Phishing Email Detection: A Hybrid Machine Learning Based on Genetic Algorithm Feature Selection,” IJACSA) International Journal of Advanced Computer Science and Applications, vol. 15, no. 8, 2024, Accessed: Oct. 09, 2025. [Online]. Available: www.ijacsa.thesai.org

[9]. B. B. Gupta, A. Gaurav, R. W. Attar, V. Arya, A. Alhomoud, and K. T. Chui, “Optimized Phishing Detection with Recurrent Neural Network and Whale Optimizer Algorithm,” Computers, Materials & Continua, vol. 80, no. 3, pp. 4895–4916, Sep. 2024, doi: 10.32604/CMC.2024.050815.

[10]. 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. 142532–142542, 2020, doi: 10.1109/ACCESS.2020.3013699