ISSN: 2093-5374 / E-ISSN: 2093-5382

Intelligent Cyber Defense: Utilizing Deep Learning for Robust Detection and Prevention of Phishing Websites

Sajidah Shahadha Mahmood[1*]

[1*]Department of Radio and Television Journalism, College of Mass Media, Al-Iraqia University, Baghdad, Iraq. sajidah.sh.mahmood@aliraqia.edu.iq, https://orcid.org/0000-0003-2010-917X

Received: March 26, 2025; Revised: May 08, 2025; Accepted: June 09, 2025; Published: June 30, 2025

Abstract

These days, with the advent of increasing transactions and communications happening over digital platforms, phishing has morphed to assume any online attacks that involve an attacker(s) posing as a legitimate entity, like banks, in most cases. This paper presents a sophisticated defence approach against phishing sites by modelling novel deep learning methods. To make it more transparent, our method employs Random Forest, Extra Trees and XGBoost models, each of which is a machine learning model with an ensemble classifier technique, LIME (Local Interpretable Model agnostic Explanations). The combination of these models, which are understood to handle complex data well, provides high detection accuracy and robustness. Ensemble methods are used to provide a more proper detection solution, which will reduce the false positive rate and false negative rates, so that better trust is maintained with your user base whilst allowing extra reliability of the system. LIME is a significant tool that gives interpretability of the decisions made by models, which in turn can increase users' trust and help developers to continuously improve their systems. Overall, our study underscores the importance of having agile cybersecurity services that can adapt as fast-moving and persistent phishing threats continue to innovate. Using such sophisticated methods provides our system with a robust and future-proof solution, which supports overcoming new phishing tactics, and being able to handle the threats of the digitalised world quickly.

Keywords: Component; Phishing Attacks, Cyber Defence Mechanism, Deep Learning Techniques, Phishing Website Detection, Ensemble Methods, Local Interpretable Model-Agnostic Explanation.

1 Introduction

In the age of digital transformation, the security of online transactions and communications is becoming a major concern for people, businesses, and government agencies (Chen et al., 2021). Phishing remains one of the most pervasive and destructive types of cyber threats (Alkhalil et al., 2021). Phishing attacks use deceptive stratagems, which malicious actors use to impersonate a legitimate authority and steal away giving information like login credentials, financial details and even personal data (Kheruddin et al., 2024). They result in great losses of money for enterprises or data breaches covering tens of millions of records, and cause irreparable damage to your standing within the organisation if you become known as someone who has allowed such a thing to happen to the company.

Despite all the various security measures that are in place today, phishing is a major threat for enterprises to reckon with (Dillon et al., 2021). The big reason is that phishing technology changes more

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 16, number: 2 (June), pp. 591-610. DOI: *10.58346/JOWUA.2025.I2.036*

*Corresponding author: Department of Radio and Television Journalism, College of Mass Media, Al-Iraqia University, Baghdad, Iraq.

quickly than any traditional security technology it can very easily bypass detection systems like blacklists or signature-based detection algorithms (Jain & Gupta, 2022). Moreover, these traditional methods often cannot keep up with the sheer number of phishing attacks that are going on all at once, which can change their patterns and targets as quickly as the weather does for clouds in spring or summer. The purpose of this research is to use machine learning techniques to build a system for phishing website detection that is more adjustable and resilient than traditional techniques (Alnemari & Alshammari, 2023).

To fight phishing attacks, one of the challenges is being able to correctly distinguish between real and fake websites (Alabdan, 2020). Phishing websites often mimic real sites very closely, making it difficult to tell which is which for both users and traditional detection systems (Zamir et al., 2020). The situation is further complicated by the continually developing nature of phishing email campaigns, which might use URL obfuscation, domain spoofing, and subtle social engineering techniques (Goenka et al., 2024). The shortcomings of traditional methods, which depend upon prescribed knowledge or fixed rules instead of real-time information exchange and updates combined with learning from experience gained in practice (Amiri-Zarandi et al., 2022), are what have sparked such an urgent need for more dynamic intelligent approaches.

This paper aims to solve the problem of phishing website detection by developing machine learning models capable of learning from extensive data and changing as new trends in phishing techniques arise (Do et al., 2022). The main objectives are to reduce the number of false positives, where real websites are falsely identified as phishing sites and false negatives, which are cases where phishing websites go undetected. Achieving this goal balance will be critical for maintaining people's trust and offering them a practicable tool for protection that does not prevent them from accessing legitimate resources on the web.

2 Aims of the Study

The objective of this study is to see how well different kinds of machine learning models can recognise phishing websites. Several machine learning algorithms are put into operation and evaluated in the research, such as Random Forest (Yang et al., 2021), Extra Trees (Anusree et al., 2021), and XGBoost classifiers (Kumar et al., 2024). These models are specifically chosen because they have performed well in dealing with intricate datasets. In addition, doing so provides higher accuracy levels when solving classification operations. This study also combines several ensemble learning methods (Bountakas & Xenakis, 2023) such as hard voting (Karim et al., 2023), soft voting (Taha, 2021) and stacked classifiers (Al-Sarem et al., 2021). Ensemble methods like these combine the predictions of multiple models to create increased predictability and robustness.

Part of the study is to use LIME (Local Interpretable Model-agnostic Explanations) to give the model's predictions a little interpretability (Hernandes et al., 2021). LIME shows what feature attributes matter most to the model-making process. Such transparency is crucial for confidence in the system being constructed, particularly for critical systems where the basis of a decision should be understood almost as much as the decision itself.

The study aims to achieve several particular results, determining the most successful machine learning systems for phishing detection, and structuring these models to minimise error rates (Do et al., 2022). Detailed comparison with the current detection means. This research is also designed to establish a normal detection system that can be constantly adjusted to match the fishing strategies as anonymous Internet users commit them.

3 Related Work

This paper (Adebowale et al., 2020) presents the Intelligent Phishing Detection System (IPDS), a hybrid model which utilises Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) algorithms in direct response to the recent sophistication of phishing attacks (Ayeblo & Faraahi, 2015). IPDS is the development of a dataset of 1 million URLs and over 10,000 pictures, which analyses the website URL, pictures, text, and frames to show robust phishing detection solutions. The system achieved an accuracy in spam detection of over 93.28% and could locate a spam site within 25 seconds on average. By leveraging the strengths of CNNs and LSTMs, the IPDS achieves greater accuracy without longer training time. The study also points out that by combining hybrid features from text, images and frames, a competent deep learning solution for phishing detection can be designed. Based on behavioural patterns, the IPDS system can identify and filter malicious websites, offering superior protection against phishing. Further work will involve developing an array of real-time web browser plugins for comprehensive online security that will detect both Trojan attacks and other kinds of malware.

In this paper (Saha et al., 2020), we talk about the spike in phishing attacks that are taking full advantage of people's dependence on digital platforms for their social and work interactions due to COVID-19, which has opened up new possibilities for cybercrime (Anitha & Dhivya, 2019; Ammi & Jama, 2023). Phishing, Phishing attacks target users' online service accounts and credentials by creating invalid-looking websites (Rishikesh et al., 2022). The usual detection strategies like blacklists or antivirus are usually not enough to prevent the evolution of these threats. In this study, first, a deep learning algorithm using a multilayer perceptron of a feed-forward neural network (FFNN) to detect phishing websites is introduced. The proposed model reached an accuracy of 95% in the training stage and obtained a performance of 93% over the held-out set from the Kaggle dataset with ten noisy attributes for each one among ten thousand webpages. Webpages are classified into phishing, suspicious and legitimate by the system with detection accuracies of 96.3% for Phishing, 90.5% for Suspicious, and safe websites, respectively (legitimate). The small difference between training and test accuracies indicates the success of our model in learning from the data (generalisation), i.e, prediction for a never-seen webpage. In future, we will work on increasing the suspicious website identification by including more layers and using advanced neural networks like backpropagation.

This paper (Elsadig et al., 2022) uniquely applies BERT to the task of phishing and uses deep learning methods in order to detect malicious URLs. To account for the more sophisticated phishing attacks exploiting unsuspecting users to reveal sensitive information, a BERT model was used by researchers in order to describe text-based features within URL paths of Phishing Site Predict Dataset We then treated these as tokens, which were subsequently used by applying NLP methods to transform them into descriptive data features. To classify URLs as they are legit or phishing, a deep convolutional neural network (CNN) was used to extract higher-layer features from the text. Experimental results showed that the proposed method was able to detect phishing URLs accurately for a large-scale public dataset consisting of 549,346 entries, with an overall accuracy rate being 96.66%. The current outcome was compared with the literature, which suggests that the proposed method can be efficient and viable for phishing detection. These results showcase the possibility of merging the feature extraction capability of BERT with plus classification power of CNN. Further work includes improving the model with dynamic feature selection as well as refining and optimising this CNN classifier model for an improved phishing detection solution.

In this paper (Lakshmi et al., 2021), the authors address the growing issue of phishing, where fake websites mimic legitimate ones to steal sensitive information. Traditional phishing detection techniques,

such as Bayesian classification, offer around 90% accuracy but struggle with large datasets. To improve detection, the authors propose a novel approach utilising 30 hyperlink features extracted from web HTML sources. They trained a supervised deep neural network using the Adam optimiser and the Listwise approach for classification. The study compared two network models, Model-1 and Model-2, varying the number of hidden units. Model-2, with fewer hidden units, demonstrated superior performance compared to Model-1. Experimental results from the Phishing Websites Data Set from the UCI repository revealed that deep learning methods outperformed traditional machine learning techniques like SVM, Adaboost, and AdaRank. Model-2 achieved up to 98.44% accuracy, surpassing other optimisers such as SGD and RMSPROP. The findings suggest that for large datasets, deep neural networks with the Adam optimiser offer a more stable and effective solution for phishing detection.

This paper (Subasi et al., 2017) addresses the challenge of phishing, where deceptive websites impersonate legitimate ones to steal users' information. While no single solution can eliminate phishing, data mining techniques present a promising approach for detection. The paper proposes an intelligent phishing detection system employing various data mining techniques to classify websites as either legitimate or phishing. Classifiers are assessed using accuracy scores, area under the ROC curve (AUC), and F-measure. Among the tested classifiers, Random Forest emerged as the most effective, achieving an accuracy of 97.36%. Its rapid execution time and efficiency make Random Forest particularly well-suited for phishing detection. The study demonstrates that Random Forest is both faster and more accurate compared to other classifiers in identifying phishing websites.

This paper (Subasi & Kremic, 2020) tackles the growing threat of phishing, which involves fraudsters setting up sham websites to pinch personal information like account passwords. Such traditional countermeasures are no longer sufficient in light of the increasing utilisation and sophistication of the Internet, a medium that has inherent security risks associated with its use. An intelligent, ensemble machine learning-based framework has been proposed in the study for the detection of phishing websites and classification of a URL as legitimate or phishing. The research evaluates classifiers with the AUC, F-measure and accuracy, finding that Adaboost with an SVM ensemble model has having highest accuracy rating of 97.61%. This shows that model learners with ensemble, like AdaBoost and Multiboost, play an important role in increasing the performance of phishing detection. In future work, we plan to study feature selection further in order to less dependence on webpage content as well as deep learning strategies toward better detection. Moreover, a mobile solution must be devised for the detection of phishing attacks have to devise because traditionally, people use this technology to browse sensitive information.

This paper (Sountharrajan et al., 2020) contributes to the current phishing research field by focusing on a serious digital security threat behaviour by deceiving bank customers into supplying confidential personal and account-related data with deceptive clone webpages of official banking websites & malicious emails (John & Ghate, 2024). The study complains that traditional methods of blacklisting is not enough and so suggests machine-learning models could help to improve the ability to detect phishing Arendt. The proposed approach uses deep learning methods, Deep Boltzmann Machines (DBM), Stacked Auto-Encoders (SAE) and Deep Neural Networks (DNN). Preprocessing and feature extraction from DBM and SAE show a reduction in the number of features by one-fold with a lower misclassification rate compared to the state-of-the-art method. A DNN is then trained for binary classification into phishing and legitimate URLs. This system can differentiate between genuine and malicious websites with a detection rate of 94% at very low false positive rates, which surpasses all other machine learning methods for the phishing phenomenon.

This paper (Alam et al., 2020) is research on an international level and sought to determine how phishing in the digital era has become a very vast threat where cybercriminals deceive users to get the confidential user credentials, as well as launch attacks such as ransomware (Seyedan et al., 2023). This study outlines a machine learning (ML) model for phishing detection with two algorithms of Random Forest (RF) and Decision Tree (DT). Using a basic dataset of phishing attacks scraped from Kaggle, the model utilises Principal Component Analysis (PCA) for feature selection and dataset normalisation. Results show that the RF algorithm outperformed in both maximum accuracy (achieving 97%) and had less variance, overfitting than the DT baselines. A confusion matrix was used to evaluate the performance, demonstrating RF's efficacy in phishing site classification. The next work will be to use CNN in IDS for more accurate prediction and detection of phishing attacks.

This paper (Korkmaz et al., 2022) addresses the problem of phishing, a widespread attack vector that is particularly threatening because it scales well to large numbers of potential victims via email and social media. Typical phishing detection techniques, such as URL analysis, are appealing due to their simplicity and speed, but often suffer from a high rate of false positives, or alternatively, may miss more attempts that are advanced attempts. This paper introduces a hybrid detection by incorporating URL and content-based features for better accuracy. The method was exercised on a High-Risk URL and Content-Based Phishing Detection Data Set from the only available web phish-catch service: Phishtank, which contains purely suspicious malicious websites. The hybrid method improved detection performance, resulting in reduced false positives on the dataset while achieving a high accuracy rate of 98.37% as revealed by experimental results with such a realistic dataset.

Table 1: Related Work

Paper	**Detection Technique**	**Dataset**	**Accuracy**	**Comments**
(Adebowale et al., 2020)	CNN + LSTM	1 million URLs, 10,000 images	93.28%	High accuracy in spam detection; fast site identification.
(Saha et al., 2020)	FFNN (Feed-forward Neural Network)	Kaggle dataset (10,000 webpages)	95% (training), 93% (test)	Accuracies: 96.3% (Phishing), 90.5% (Suspicious), Rest (Legitimate). Good generalisation performance.
(Elsadig et al., 2022)	BERT + CNN	549,346 URLs	96.66%	Effective use of BERT for feature extraction and CNN for classification.
(Lakshmi et al., 2021)	Deep Neural Network (DNN)	UCI Phishing Data Set	98.44%	Superior performance compared to traditional methods.
(Subasi et al., 2017)	Random Forest	Various datasets	97.36%	Efficient and accurate, with faster execution compared to other classifiers.
(Subasi & Kremic, 2020)	Adaboost + SVM Ensemble	Various datasets	97.61%	High accuracy; ensemble models enhance detection performance.
(Sountharrajan et al., 2020)	DBM + SAE + DNN	Various phishing datasets	94%	Effective with low false positive rates, good performance in distinguishing phishing sites.
(Alam et al., 2020)	RF + DT + PCA	Kaggle dataset	97%	RF outperforms DT; PCA used for feature selection.
(Korkmaz et al., 2022)	Hybrid (URL + Content-based)	Phishtank dataset	98.37%	High accuracy; hybrid approach improves detection and reduces false positives.

Table 1 summarises different phishing detection methods disclosed in various studies and their performance with respect to accuracy. Papers (Adebowale et al., 2020) and (Saha et al., 2020) present highly accurate outcomes using advanced machine learning models, at 93.28% and a maximum of 95%, respectively. Paper (Elsadig et al., 2022) combines BERT and CNN to present a very high accuracy of 96.66%, which outlines the effectiveness of the method in feature extraction and classification. With deep learning and Random Forest methods proving highly accurate, Papers (Lakshmi et al., 2021) and (Subasi et al., 2017) record high accuracies at 98.44% and 97.36%, respectively. Paper (Subasi & Kremic, 2020) records a high accuracy of 97.61% with an ensemble approach utilising Adaboost and SVM. Conversely, an accuracy of 94% using a combination of DBM and SAE and DNN, Paper (Sountharrajan et al., 2020) relates a highly accurate outcome too. Finally, paper (Korkmaz et al., 2022) presents the most accurate outcome of 98.37%, crediting the high profile to a hybrid method encompassing URL and content-based features. All the methods demonstrate high accuracy; hence, hybrid and advanced deep learning methods present authentic performance for detection.

4 Methodology

This approach structures the methodology to identify and harvest these phishing campaigns, thereby making it extremely effective. As shown in Figure 1, this begins with an exhaustive data pre-processing phase in which the dataset is loaded into a pandas DataFrame for easier manipulation (Kempter, 2024). The categorical variables are converted into a Numerical format, and the Numerical Features are scaled to standardise data (Dinh et al., 2021), which increases the Performance of Models. Data is separated into features and target variables, and then an 80-20 split is used to create a training set such that the model evaluation remains realistic (Birba, 2020).

Extra Trees, Random Forest, Decision Tree and XGBoost, together with Gradient Boosting SVM, MLP, are trained on features for classification prediction of models as accuracy, precision and recall (Mithra Raj & Arul Jothi, 2022). For better prediction accuracy, ensemble methods are used with the top 3 models (commonly XGBoost, Extra Trees and Random Forest), which perform at their best. The ensemble thereby capitalises on the different strengths of each model whilst minimising their individual weaknesses (Maddireddy & Maddireddy, 2022).

The methodology includes utilising LIME-Local Interpretable Model-agnostic Explanations to explain predictions made by the model, clarifying which factors are affecting decisions. This can be extremely useful when it comes to interpreting complex models in a way that is consistent with the domain knowledge. The large-scale experimentation ensures that we have generalizability and reliability for results by applying the well-grounded methodology comprehensively on multiple datasets. This standardised method makes the model a useful asset in recognition and battling phishing campaigns across different scenarios and dataset sources (Nirmal et al., 2021).

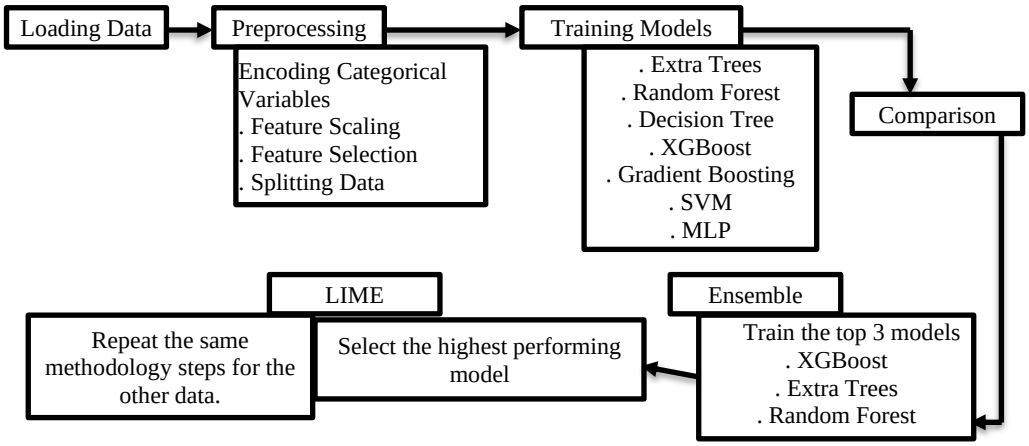

Figure 1: Proposed Methodology For Phishing Website Detection Using a Hybrid Machine Learning Framework

4.1 Dataset Overview

- **First Dataset**

The dataset (Web page Phishing Detection Dataset, 2024) is thoroughly designed to benchmark machine learning models targeting phishing detection. These include 11,430 URLs, each with 87 features. It is worth mentioning that the dataset is also balanced, with 50% of URLs containing phishing and the other 50% containing legitimate ones. Such datasets are extremely important in ensuring that the modelling and testing of the model are done evenly. The dataset features are divided into three categories. One hundred and ten structural features denote 56 structural f read, indicating the URL's length, the "." and "-" count as special characters such as "@" and "&," "//" presence and IP address. This is important because some of the patterns will be denoted by free, using a huge amount of punctuation or unusual URL building. There are also 24 Content-based features denoted in the dataset. This involves examining the webpages linked to the URLs. Text content and images can be used to determine if the website has identical content as genuine sites or uses copied or unstructured content. Finally, seven features from external services verifications. Such features are the last piece of the cake, adding features such as why the hosting details, relatives, and reputation are primary to a URL analysis, which grants the URL's credibility component. The dataset this of validated. No missing data or functional characteristics are not functioning; the retrieval is verified as not to be lost, ensuring that the data is consistent. To explore and expand the capability of creating software applications that can produce more capable and efficient phishing detection devices, internet protection will be significantly increased.

- **Second Dataset**

Phishing Dataset for Machine Learning, this data (Aljammal et al., 2023) set is geared towards helping the cybersecurity community develop tools specifically designed to block phishing attempts, perhaps as it remains one of the simplest ways in which attackers can phish and compromise numerous individuals who may give a lot of private information. Type: Dataset Validated through public access to data. This dataset consists of 48 features extracted from about 10,000 webpages featuring phishing and legitimate sites. Data were not collected on the same date as are between January/June 2015 and May-June 2017. The features were extracted with an enhanced technique based on the use of a browser automation framework, Selenium WebDriver, for more accurate and robust feature extraction in comparison to

traditional parsing methods relying heavily on regular expressions. This way, the resulting dataset is both thorough and representative, prepared to serve for researchers in anti-phishing fields as valuable reference. Such a dataset is also useful for researchers who are in favour of working on analysing phishing features, quick proof of concept experiments, while comparing it as a benchmark against their phishing classification models, enabling the development of stronger anti-phishing tools and strategies.

4.2 Data Preparation and Preprocessing

The process starts with the data preparation through loading the dataset into a simple data frame capable of efficient manipulation and analysis, such as pandas DataFrame (Gupta & Bagchi, 2024). In the 'status' column, categorical variables are put as numerical values with LabelEncoder to use them in machine learning algorithms (Sree et al., 2021). Followed by scaling the numeric features so that all of these will be consistent, this step is crucial, especially when fitting models on features with a wide magnitude. Since the 'url' column has nothing to do with predictive modelling, it is dropped from our dataset. The dataset is then split into features (X) and the target variable (y), where -1 values in the y are set to zero, which many classification algorithms require that outputs be non-negative. This preprocessing helps in making the data clean, well formatted and prepared for machine learning model training so as to give a better and more accurate analysis in further steps.

4.3 Model Training and Comparison

Phishing detection was performed using various machine learning models, which were trained and evaluated following data preparation (Alnemari & Alshammari, 2023). Among these models, the Extra Trees Classifier was employed to enhance accuracy by generating numerous decision trees and aggregating their predictions to mitigate overfitting. A more advanced approach is the Random Forest Classifier, which incorporates bootstrapping and random feature selection, along with other refinements, to improve generalisation.

The Decision Tree Classifier is simple and easy to interpret; it splits data by the value of features, so it finds a clear decision tree structure. XGBoost and Gradient Boosting Classifiers: While XGBoost has gained a large following in recent years for its high performance on complex tasks that require much data, it is still an algorithm group well designed to build models sequentially based on the classification of errors uncovered by previous ones. Support Vector Machine (SVM) Classifier helps in optimising class separation within the feature space, which leads to enhanced performance, but mainly with high-dimensional data.

Finally, the Multi-Layer Perceptron (MLP) Classifier is a type of neural network with various connected layers that allow it to capture more complex patterns, thus making it appropriate for cases in which attributes have nonlinear relationships. The training set is used to train each model and test its accuracy, precision, recall, and F1-score on the testing set. The full examination is aimed at determining the best model for phishing detection, which should be robust and accurate to work in deployment.

4.4 Comparison and Ensemble Methods

The performance of the trained machine learning models is evaluated using different evaluation metrics such as accuracy, precision, recall and F1-score. These metrics in combination present a detailed picture of the strengths and weaknesses of every model type, so, as is always important when working with data, choose the highest performing model. So, Accuracy checks whether the model is correct in total, Precision calculates the proportion of true positive predictions compared to all predicted cases as Positive, Recall checks whether anything we are relevant, it should identify that instance, and F1-Score provide a balanced approach between precision & recall.

To improve overall performance, an ensemble approach is used. This technique enhances the prediction of individual models; thus, each model contributes to the result and should make it more accurate. The ensemble method necessarily decreases the probability of errors during prediction and provides more trust than standard models. The final model fuses the constituent models to leverage all of their different perspectives and decision-making capabilities, so this hybrid approach has many benefits.

4.5 Enhancing Model Transparency with LIME

The methodology incorporates LIME (Local Interpretable Model-agnostic Explanations) for interpretability alongside training and evaluating multiple machine learning models. LIME explains what exactly contributed to making the given predictions, thus explaining what arguments are accounting for model decisions.

LIME works, as it points out to be approximates the model locally around predictions and generates interpretable surrogate models, which mimic the behaviour of a complex original model in a smaller region. This provides insight into how much each feature contributes to the prediction and makes the decision-making process transparent. Understanding why the model made each prediction is also important for critical applications, such as phishing detection.

Interpretability through LIME helps the stakeholders, who include security analysts, decision-makers, understand why a model predicted, thereby bringing in transparency. That insight can then inform detection refinement, systematic reviews of possible vulnerabilities, and facilitation of improved security polices. In addition, it helps the model developer to communicate how the model works with non-technical business stakeholders, and this increases trust in putting AI-based solutions into a production environment.

Using LIME in the methodology ensures that all machine learning models not only predict correctly but also provide explainability and transparency. It is this mix of high performance and interpretability that Real Time Email uses to create a more robust, accurate phishing detection system, which results in better security outcomes for the users.

5 Experiment Results

5.1 Experiment Results of the First Dataset

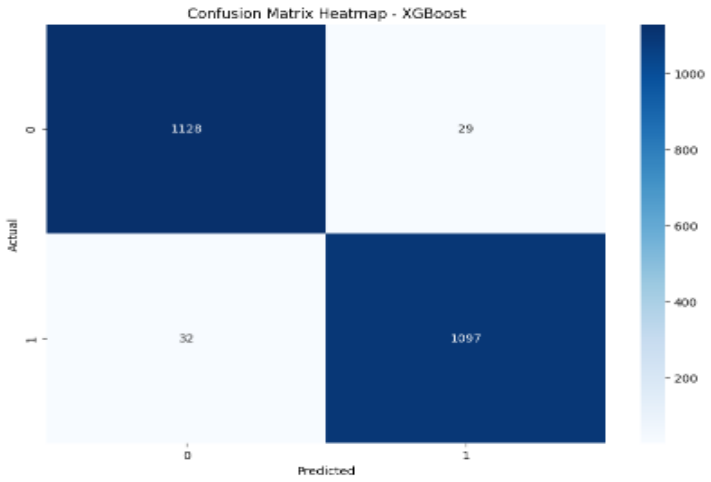

Figure 2: Confusion Matrix of XGBoost

In Figure 2, the confusion matrix of the XGBoost applied model on the provided dataset demonstrates good classification performance. It got 1,128 instances correct as class 0 (true negatives), and it also correctly predicted 1,097 cases as class 1. Granted, there were 29 instances incorrectly classified as class-1 when they should have been labelled properly (false positives) and another 32 cases where, even though the instance belonged to class-O, were misclassified as false positives. On the other hand, this matrix has very high values at its diagonal (1,128 and 1,097), which means that it has done a great job of classifying both classes correctly. The low numbers of false positives and negatives (29 & 32) indicate that this may also be a robust model in terms of dealing with classification errors on the dataset at hand.

5.2 Comparison Between Models Before Using the Ensemble

	Model	Accuracy	Recall	Precision	F1 Score	Error Rate	Training Time (s)
3	XGBoost	0.973316	0.971656	0.974245	0.972949	0.026684	0.780205
0	Extra Trees	0.969379	0.958370	0.979186	0.968666	0.030621	1.345164
1	Random Forest	0.969379	0.962799	0.974888	0.968806	0.030621	2.032022
6	MLP	0.963692	0.962799	0.963652	0.963226	0.036308	41.404018
5	SVM	0.963255	0.961027	0.964444	0.962733	0.036745	5.033155
4	Gradient Boosting	0.959318	0.959256	0.958407	0.958831	0.040682	7.388573
2	Decision Tree	0.935258	0.936227	0.932921	0.934571	0.064742	0.250767

Figure 3: Comparison Between the Models' Results Before Using the Ensemble

Figure 3 visualises the analysis of machine learning models with regard to accuracy, recall, precision, F1 score, error rate and Training Time. Finally, the XGBoost model outperforms all models at least in this data set and with the highest accuracy of 0.973316, recall (0.971656), precision (0.974245), and F1 score (0.972949). It has the lowest error rate as well, of 0.026684, and it trained relatively fast at 0.780205 seconds.

The Extra Trees and the Random Forest models give very close performances, with each one yielding an accuracy of 0.969379 as well as some recall, precision and F1-scores on the same levels. They also both have the same error rate at 0.030621, though Extra Trees trains faster.

The MLP model has an accuracy of 0.963692, with the highest classification error, but also the longest training time. SVM again gives better prediction scores and time to train than MLP.

Gradient Boosting trails the best models in accuracy and error rates, though it is still a strong performer across its comprehensiveness. The accuracy of the Decision Tree is lower, and errors are higher, but it takes less time to train.

Overall, XGBoost is a leader in most of these metrics with reasonable training time as well, but Extra Trees and Random Forest are strong candidates too. MLP and SVM all give better performances but demand more time to be trained as opposed to the edited dataset. The Decision Tree model, trained immediately but lagged well behind in both accuracy and other metrics.

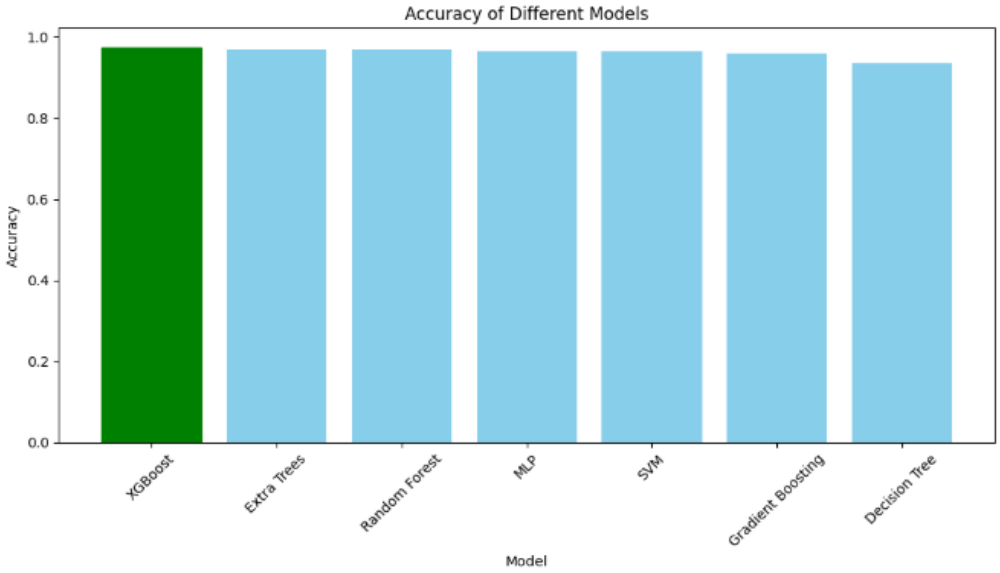

Figure 4: Accuracy of Different Models

Figure 4 shows the effectiveness of different machine learning models. It is followed by the dark green bar indicating XGBoost to be less accurate than the other three models, but still almost 100% correct. All other models, Extra Trees, Random Forest, MLP, SVM, Gradient Boosting, also have high accuracy since all gradient light blue bars are almost similar to XGBoost's. Extra Trees and Random Forest are the most accurate models; they produce similar results, followed by MLP, SVM, which have very close performances. These models have only slightly less accuracy compared to Gradient Boosting. The light blue bar refers to the Decision Tree model, achieving the highest level of accuracy but being comparatively less accurate than all the models. This should reflect in the colored bars below, where you will see that XGBoost has better accuracy more often than other models.

5.3 Comparison Between Models After Using the Ensemble

	Model	Accuracy	Recall	Precision	F1 Score	Error Rate
5	Stacking Ensemble	0.975503	0.975503	0.975537	0.975501	0.024497
4	Soft Voting Ensemble	0.975066	0.975066	0.975093	0.975064	0.024934
0	XGBoost	0.973316	0.973316	0.973318	0.973315	0.026684
3	Hard Voting Ensemble	0.973316	0.973316	0.973373	0.973313	0.026684
1	Extra Trees	0.969379	0.969379	0.969578	0.969372	0.030621
2	Random Forest	0.969379	0.969379	0.969445	0.969375	0.030621

Figure 5: Comparison Between Models Results After Using the Ensemble

Figure 5 presents a comparison of machine learning models, emphasising the advantages of ensemble methods. The Stacking Ensemble model stands out with the highest accuracy (0.975503), recall (0.975503), precision (0.975537), F1 score (0.975501), and the lowest error rate (0.024497). The Soft Voting Ensemble closely follows with an accuracy of 0.975066 and a slightly higher error rate of 0.024934.

As an individual model, XGBoost performs strongly with an accuracy of 0.973316 and an error rate of 0.026684, comparable to the Hard Voting Ensemble's metrics. Extra Trees and Random Forest models exhibit slightly lower accuracy (0.969379) and higher error rates (0.030621) but still maintain solid performance.

Based on this analysis, we selected the top three models to work with: XGBoost, Extra Trees, and Random Forest. These models showed robust individual performance and form a strong foundation for further ensemble methods.

In summary, ensemble methods, particularly Stacking and Soft Voting, enhance model performance, outperforming individual models like XGBoost, Extra Trees, and Random Forest in accuracy and error rate. Our focus on XGBoost, Extra Trees, and Random Forest ensures we utilise the best-performing models for our tasks.

5.4 LIME Results for XGBClassifier Model

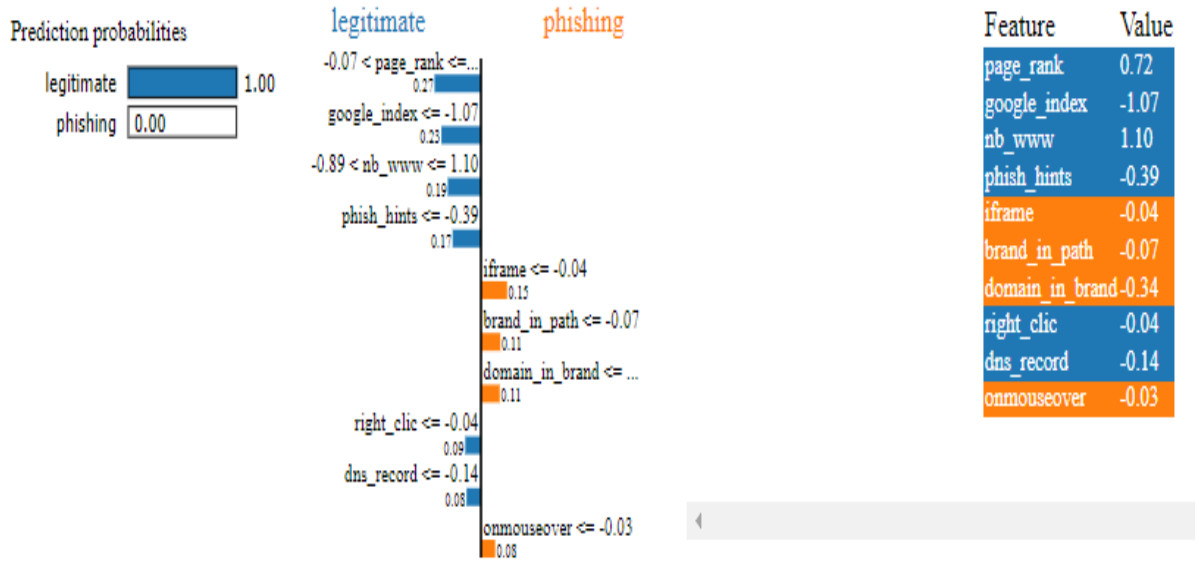

Figure 6: LIME Interpretability Results for the XGBClassifier Model

As illustrated in Figure 6, analysing the LIME results indicates influential and insightful factors influencing the predictions of the XGBClassifier for differentiating legitimate and phishing websites. The analysis shows that the model systematically considers certain essential features, and for instance, the score for page rank is 0.72, which means that higher values strongly suggest that the website is legitimate. This is because reputable websites usually post higher search engine rankings to attract more users. Additionally, the score for the existence of the website in Google's index (-1.07) is a strong positive influence. The number of occurrences of 'www' is 1.10, and the presence of specific elements relating to phishing (0.39) is also a powerful positive indicator. While influencing features such as iframe (-0.04), brand in path (-0.07), domain in brand (-0.34), right click (-0.04), DNS record (-0.14), and onmouseover (-0.03) features are weaker it is clear that they combine their influences to enhance the model's ability to differential. In conclusion, the LIME results have shown that the XGBClassifier has captured critical aspects of the legitimate and phishing websites by concentrating on the authority of the website, the structure of the website and the elements that seem suspicious, which are relevant insights to detect illegal activities on the internet.

5.5 Experiment Results of the Second Dataset

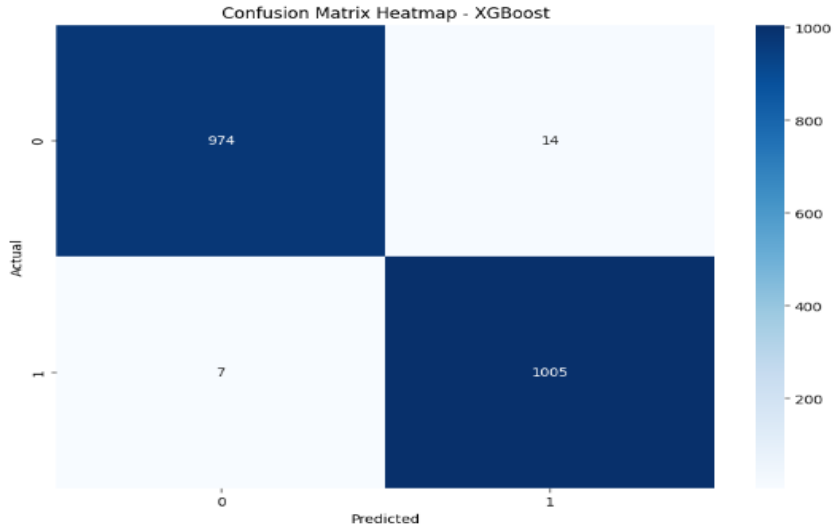

Figure 7: Confusion Matrix Heatmap for the XGBoost Model on the Second Dataset

A confusion matrix for the XGBoost model, Figure 7, highlights actual and predicted classifications of benign, phishing websites. So the matrix shows that 974 legitimate sites were correctly identified using this model (TNs), and for phishing websites, there are 1005 TP. It improperly categorised 14 real sites as phishers, i.e., false positives and 7 phishing pages identified were actually legitimate (false negatives). These results show significant accuracy with a lower number of misclassifications. The true positive and true negative counts are way higher than the rest; thus illustrating that the model does an excellent job in correctly identifying a Phishing website, but not avoiding legitimate ones being labelled as such. The concentration of colours in the heatmap makes it clear that a High number of correct classifications compared with incorrect classified, so visually we can easily say the model is working well. Moreover, this model outperforms all other evaluated models in terms of robust accuracy and well-calibrated detection of online fraud.

5.6 Comparison Between Models Before Using the Ensemble

	Model	Accuracy	Recall	Precision	F1 Score	Error Rate	Training Time (s)
3	XGBoost	0.9895	0.993083	0.986261	0.989660	0.0105	0.944428
0	Extra Trees	0.9840	0.980237	0.988048	0.984127	0.0160	0.836158
1	Random Forest	0.9825	0.983202	0.982231	0.982716	0.0175	1.221421
4	Gradient Boosting	0.9810	0.984190	0.978389	0.981281	0.0190	2.192469
6	MLP	0.9770	0.972332	0.982036	0.977160	0.0230	18.721803
2	Decision Tree	0.9705	0.972332	0.969458	0.970893	0.0295	0.125725
5	SVM	0.9655	0.971344	0.960899	0.966093	0.0345	0.947258

Figure 8: Comparison Between Models' Results of the Second Dataset

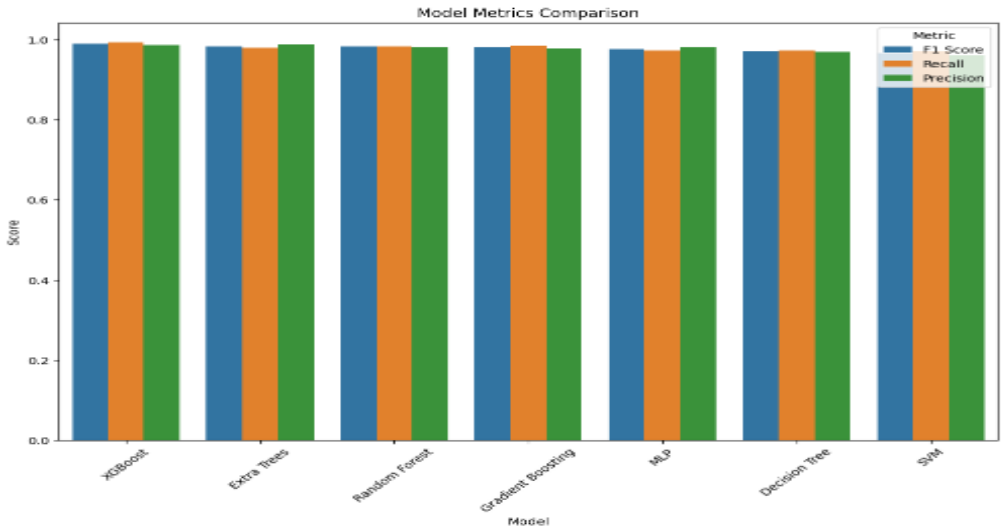

Figure 9: Model Metrics Comparison

Figures 8 and 9 provide a full comparison of several models' performance on the second dataset. They can help analyse each model's performance by distinguishing the most critical metrics, such as accuracy, recall, precision, F1 score, error rate, and training time. The model for the given dataset with a high level of all these metrics is XGBoost. This model demonstrated an accuracy of 98.95%, recall of 99.31%, precision of 98.63%, and F1 score of 98.97%; error rate of 0.0105, and training time of 0.944 sec. Extra trees and Random Forest also have good statistics. Gradient boosting and MLP have slightly lower results. Decision Tree and SVM are not much less efficient, but noticeable indicators and relatively higher error rates determine attractiveness as an instrument. These figures are confirmed by the bar chart in Figure 8. This model has the best results in all metrics, which allows us to choose it. The model that can most accurately determine the difference between legitimate and phishing websites in this dataset is XGBoost.

5.7 Comparison Between Models Before Using the Ensemble for the Second Dataset

	Model	Accuracy	Recall	Precision	F1 Score	Error Rate	Training Time (s)
3	XGBoost	0.9895	0.993083	0.986261	0.989660	0.0105	0.944428
0	Extra Trees	0.9840	0.980237	0.988048	0.984127	0.0160	0.836158
1	Random Forest	0.9825	0.983202	0.982231	0.982716	0.0175	1.221421
4	Gradient Boosting	0.9810	0.984190	0.978389	0.981281	0.0190	2.192469
6	MLP	0.9770	0.972332	0.982036	0.977160	0.0230	18.721803
2	Decision Tree	0.9705	0.972332	0.969458	0.970893	0.0295	0.125725
5	SVM	0.9655	0.971344	0.960899	0.966093	0.0345	0.947258

Figure 10: Model Metrics Comparison

The figure 10 presents the performance metrics for 6 different machine learning models (XGBoost, Extra Trees, Random Forest Gradient Boosting), MLP, Decision Tree and SVM on a concrete dataset The result of the performance metrics indicates that XGBoost outperforms AdaBoost, Binary Relevance and Chain Classifier, with Accuracy (0.9895), Recall (0.9930), Precision (9863) F1 Score 09897 indicating an low error rate as: Extra Trees follows close behind with a solid performance as well. It is simple, and it has the hardest effect on training time, but in other metrics like accuracy, the Decision Tree has mediocre performance. In contrast, MLP shows much more training time but lower accuracy than the tree-based models.

5.8 Comparison Between Models After Using an Ensemble for the Second Dataset

	Model	Accuracy	Recall	Precision	F1 Score	Error Rate
0	XGBoost	0.9895	0.9895	0.989523	0.989499	0.0105
5	Stacking Ensemble	0.9895	0.9895	0.989539	0.989499	0.0105
4	Soft Voting Ensemble	0.9885	0.9885	0.988523	0.988499	0.0115
3	Hard Voting Ensemble	0.9880	0.9880	0.988007	0.988000	0.0120
1	Extra Trees	0.9840	0.9840	0.984033	0.984001	0.0160
2	Random Forest	0.9825	0.9825	0.982500	0.982500	0.0175

Figure 11: The Results of the Models for the Second Dataset Before Using the Ensemble

Figure 11 shows the comparison of performance metrics on a dataset between several models (including ensemble methods). The best results in terms of Accuracy, Recall, Precision and F1-score were reported for stacking Ensemble: 0.9895 (Accuracy), 0.9895 (Recall), 0.9895(Precision), 0 practice error rate; Followed by Soft Voting Ensemble, which was not far behind and returned slightly lower metrics. Hard Voting Ensemble further decreased its performance by a small margin. For example, the ensemble methods had superior skill during both training and testing cycles compared to models run individually, like Extra Trees or Random Forest.

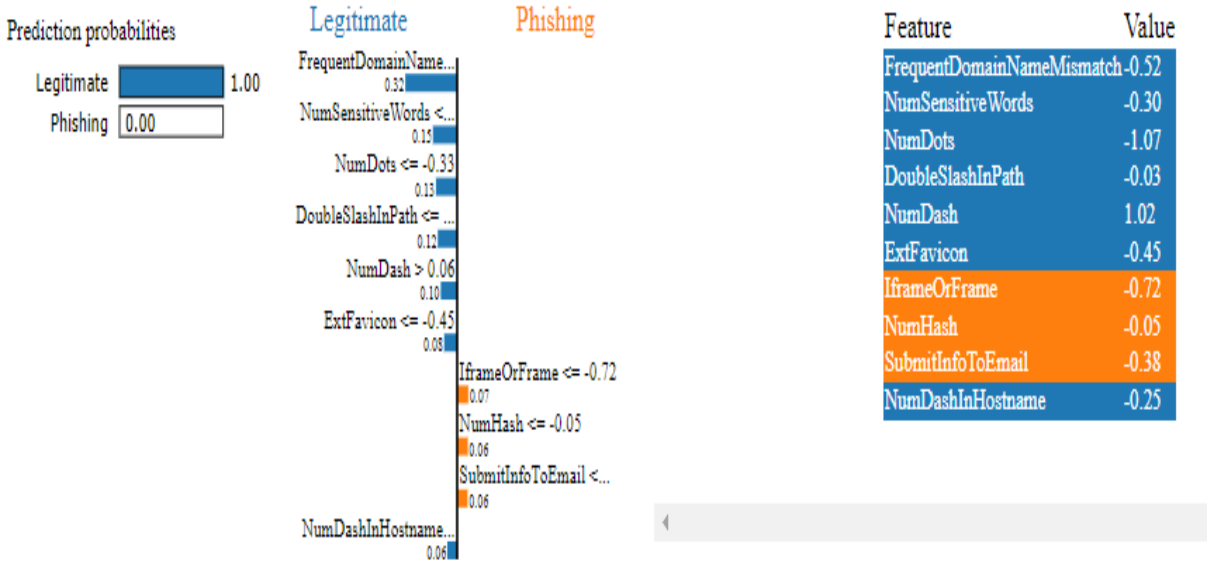

Figure 12: LIME Results for XGBClassifier Model for the Second Dataset

For the XGBClassifier model, LIME results show in Figure 12 that the domain name is an important feature in predicting the legitimacy of a website (domain name has the highest positive class weight), followed by the number of sensitive words and the dot count. These features have a positive distribution, meaning that they increase the chances of being classified as phishing. In contrast, number strength means a website is labelled as real and assigns negative values to features such as the lack of iframes or frames and classes. These SHAP values represent the influence of each feature on a prediction.

5.9 Compare with the Related Works

This comparison of results with related works shows the effectiveness and competitiveness of models in phishing detection. In particular, enabling ensemble techniques leads to high accuracy, precision, recall and F1 scores that are even better than most numbers reported in other works. On the second dataset, the

use of XGBoost, ensemble models reach an accuracy up to 98.95% topping many benchmarking methods listed in the literature. Better detection performance has been demonstrated by advanced ensemble methods such as Stacking and Voting, thus proving the strength and reliability of this approach.

Table 2: Comparison of Proposed Model with Related Works

Paper/Model	Detection Technique	Dataset	Accuracy	Comments
(Chen et al., 2021)	CNN + LSTM	1 million URLs, 10,000 images	93.28%	High accuracy in spam detection; fast site identification.
(Ayeblo & Faraahi, 2015)	FFNN (Feed-forward Neural Network)	Kaggle dataset (10,000 webpages)	95% (training), 93% (test)	Accuracies: 96.3% (Phishing), 90.5% (Suspicious), Rest (Legitimate). Good generalisation performance.
(Kheruddin et al., 2024)	BERT + CNN	549,346 URLs	96.66%	Effective use of BERT for feature extraction and CNN for classification.
(Seyedan et al., 2023)	Deep Neural Network (DNN)	UCI Phishing Data Set	98.44%	Superior performance compared to traditional methods.
(Jain & Gupta, 2022)	Random Forest	Various datasets	97.36%	Efficient and accurate, with faster execution compared to other classifiers.
(Rishikesh et al., 2022)	Adaboost + SVM Ensemble	Various datasets	97.61%	High accuracy; ensemble models enhance detection performance.
(Alabdan, 2020)	DBM + SAE + DNN	Various phishing datasets	94%	Effective with low false positive rates, good performance in distinguishing phishing sites.
(Anitha & Dhivya, 2019)	RF + DT + PCA	Kaggle dataset	97%	RF outperforms DT; PCA used for feature selection.
(Goenka et al., 2024)	Hybrid (URL + Content-based)	Phishtank dataset	98.37%	High accuracy; hybrid approach improves detection and reduces false positives.
Our Work	**Stacking Ensemble**	First Dataset	**97.55%**	High accuracy and reliable performance on the first dataset.
Our Work	**XGBoost**	Second Dataset	**98.95%**	Superior performance with a low error rate on the second dataset.

A summary table 2 comparing the performance of different detection methods with that obtained is provided as a combined result. The results of the Stacking Ensemble model for the first dataset and XGBoost for the second dataset suggest a high degree of accuracy as well as reliability, which may provide competitive or superior performance from existing methods. It shows how effective phishing detection methodologies are.

6 Conclusion

Phishing attacks are becoming more frequent because of the increase in online transactions these days, and attackers can replicate a legitimate entity to gain access to sensitive information. Legacy detection solutions are inadequate against ever-changing methods of attacks, demanding sophisticated cyber defence measures tailored to contemporary threats.

This study demonstrates that deep learning methodologies can be helpful to improve phishing detection systems. The study introduces the use of Random Forest, Extra Trees and XGBoost to traditional machine learning models that improve accuracy and robustness through ensemble learning mechanisms. Using LIME along with these models makes the virus scanner transparent, and it is a critical requirement for cybersecurity applications to have transparency in what decisions are being made. These results demonstrate that the proposed approaches are capable of outperforming classical phishing detection mechanisms, which typically use static and defined rules leading to easy obsoletes.

This is a particularly important reduction because it indicates that the detection system is relatively balanced and capable of discriminating between legitimate websites and phishing ones with high accuracy. Such balance is fundamental not only to keep security hacking and data breaches under control, but also in the fact that permitted user activities are wrongly marked as a threat, which will reduce users' trust.

This study makes two contributions: first, to enhance the fraud detection using deep learning and ensemble methods; second, by explaining to users, trust and regulatory validity, why model interpretability is very important. The proposed system is especially advantageous in the adaptive phishing internet research scope since it can easily change and improve regardless of what new techniques cybercriminals have up their sleeves.

Future work will concentrate on improving real-time detection efficacy while also increasing the model's adaptability to new and evolving forms of phishing. Moreover, increasing the dataset size and capturing a variety of real-time Phishing scenarios will increase its accuracy and adaptability. In the end, this work lays excellent groundwork for building holistic cybersecurity strategies capable of rapidly adapting to a diverse set of digital threats.

References

[1] Adebowale, M. A., Lwin, K. T., & Hossain, M. A. (2020). Intelligent phishing detection scheme using deep learning algorithms. *Journal of Enterprise Information Management, 36*(3), 747–766. http://dx.doi.org/10.1108/JEIM-01-2020-0036

[2] Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. *Future internet, 12*(10), 168. https://doi.org/10.3390/fi12100168.

[3] Alam, M. N., Sarma, D., Lima, F. F., Saha, I., Ulfath, R.-E.-, & Hossain, S.. Phishing Attacks Detection using Machine Learning Approach. *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT). IEEE.* https://doi.org/10.1109/ICSSIT48917.2020.9214225

[4] Aljammal, A. H., taamneh , S. ., Qawasmeh, A. ., & Bani Salameh, H. (2023). Machine Learning Based Phishing Attacks Detection Using Multiple Datasets. *International Journal of Interactive Mobile Technologies (iJIM), 17*(05), pp. 71–83. https://doi.org/10.3991/ijim.v17i05.37575

[5] Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science, 3*, 563060. https://doi.org/10.3389/fcomp.2021.563060.

[6] Alnemari, S., & Alshammari, M. (2023). Detecting phishing domains using machine learning. *Applied Sciences, 13*(8), 4649. https://doi.org/10.3390/app13084649

[7] Al-Sarem, M., Saeed, F., Al-Mekhlafi, Z. G., Mohammed, B. A., Al-Hadhrami, T., Alshammari, M. T., ... & Alshammari, T. S. (2021). An optimised stacking ensemble model for phishing website detection. *Electronics, 10*(11), 1285. https://doi.org/10.3390/electronics10111285

[8] Amiri-Zarandi, M., Hazrati Fard, M., Yousefinaghani, S., Kaviani, M., & Dara, R. (2022). A platform approach to smart farm information processing. *Agriculture, 12*(6), 838. https://doi.org/10.3390/agriculture12060838

[9] Ammi, M., & Jama, Y. M. (2023). Cyber Threat Hunting Case Study using MISP. *Journal of Internet Services and Information Security, 13*(2), 1-29. https://doi.org/10.58346/JISIS.2023.I2.001

[10] Anitha, G., & Dhivya, R. (2019). Denial of Service Attack in Cyber Crime Security. *International Journal of Advances in Engineering and Emerging Technology, 10*(4), 1–13.

[11] Anusree, A., Jose, B., Anilkumar, K., & Lee, O. T. (2021, October). Phishing detection using extra trees classifier. In 2021 5th International Conference on Information Systems and Computer Networks (ISCON) (pp. 1-6). *IEEE.* http://dx.doi.org/10.1109/ISCON52037.2021.9702372

[12] Ayeblo, Y. N., & Faraahi, A. (2015). A Survey of the Solutions to Detect and Deal with File Injection Attacks in Web Sites through Access to Web Server Shared Resources. *International Academic Journal of Science and Engineering, 2(*2), 234–248.

[13] Birba, D. E. (2020). *A Comparative study of data splitting algorithms for machine learning model selection.*

[14] Bountakas, P., & Xenakis, C. (2023). Helphed: Hybrid ensemble learning for phishing email detection. *Journal of network and computer applications, 210,* 103545. https://doi.org/10.1016/j.jnca.2022.103545

[15] Chen, C. L., Lin, Y. C., Chen, W. H., Chao, C. F., & Pandia, H. (2021). Role of the government to enhance digital transformation in small service businesses. *Sustainability*, *13*(3), 1028. https://doi.org/10.3390/su13031028.

[16] Dillon, R., Lothian, P., Grewal, S., & Pereira, D. (2021). Cybersecurity: evolving threats in an ever-changing world. In Digital Transformation in a Post-COVID World (pp. 129-154). *CRC Press.* http://dx.doi.org/10.1201/9781003148715-7.

[17] Dinh, D. T., Huynh, V. N., & Sriboonchitta, S. (2021). Clustering mixed numerical and categorical data with missing values. *Information Sciences, 571,* 418-442. https://doi.org/10.1016/j.ins.2021.04.076

[18] Do, N. Q., Selamat, A., Krejcar, O., Herrera-Viedma, E., & Fujita, H. (2022). Deep learning for phishing detection: Taxonomy, current challenges and future directions. *IEEE Access, 10,* 36429-36463. http://dx.doi.org/10.1109/ACCESS.2022.3151903

[19] Elsadig, M., Ibrahim, A. O., Basheer, S., Alohali, M. A., Alshunaifi, S., Alqahtani, H., ...Nagmeldin, W. (2022). Intelligent Deep Machine Learning Cyber Phishing URL Detection Based on BERT Features Extraction. *Electronics, 11*(22), 3647. https://doi.org/10.3390/electronics11223647

[20] Goenka, R., Chawla, M., & Tiwari, N. (2024). A comprehensive survey of phishing: Media, intended targets, attack and defence techniques and a novel taxonomy. *International Journal of Information Security, 23*(2), 819-848. http://dx.doi.org/10.1007/s10207-023-00768-x

[21] Gupta, P., & Bagchi, A. (2024). Introduction to Pandas. In Essentials of Python for Artificial Intelligence and Machine Learning (pp. 161-196). *Cham: Springer Nature Switzerland.* http://dx.doi.org/10.1007/978-3-031-43725-0_5

[22] Hernandes, P. R. G., Floret, C. P., De Almeida, K. F. C., Da Silva, V. C., Papa, J. P., & Da Costa, K. A. P. (2021, December). Phishing detection using URL-based XAI techniques. In 2021 IEEE Symposium Series on Computational Intelligence (SSCI) (pp. 01-06). *IEEE.* http://dx.doi.org/10.1109/SSCI50451.2021.9659981

[23] Jain, A. K., & Gupta, B. B. (2022). A survey of phishing attack techniques, defence mechanisms and open research challenges. *Enterprise Information Systems, 16*(4), 527-565. https://doi.org/10.1080/17517575.2021.1896786

[24] John, B., & Ghate, A. D. (2024). Digital Risk Management: A Study of How Firms Mitigate Digital Risks and Threats. *Indian Journal of Information Sources and Services, 14*(4), 16–21. https://doi.org/10.51983/ijiss-2024.14.4.03

[25] Karim, A., Shahroz, M., Mustofa, K., Belhaouari, S. B., & Joga, S. R. K. (2023). Phishing detection system through a hybrid machine learning based on URL. *IEEE Access, 11,* 36805-36822. https://doi.org/10.1109/ACCESS.2023.3252366

[26] Kempter, Y. (2024). *ML Data Processing on Relational Databases (Master's thesis, ETH Zurich)*. https://doi.org/10.3929/ethz-b-000677800.

[27] Kheruddin, M. S., Zuber, M. A. E. M., & Radzai, M. M. M. (2024). Phishing Attacks: Unraveling Tactics, Threats, and Defenses in the Cybersecurity Landscape. *Authorea Preprints.* https://doi.org/10.22541/au.170534654.48067877/v1.

[28] Korkmaz, M. ., Kocyigit, E. ., Sahingoz, O. K., & Diri, B. (2022). A Hybrid Phishing Detection System Using Deep Learning-based URL and Content Analysis. *Elektronika Ir Elektrotechnika*, *28*(5), 80-89. https://doi.org/10.5755/j02.eie.31197

[29] Kumar, P., Antony, K., Banga, D., & Sohal, A. (2024). PhishNet: A Phishing Website Detection Tool using XGBoost. *arXiv preprint arXiv:2407.04732.* https://doi.org/10.48550/arXiv.2407.04732

[30] Lakshmi, L., Reddy, M. P., Santhaiah, C., & Reddy, U. J. (2021). Smart Phishing Detection in Web Pages using Supervised Deep Learning Classification and Optimisation Technique ADAM. *Wireless Pers. Commun., 118*(4), 3549–3564. https://doi.org/10.1007/s11277-021-08196-7.

[31] Maddireddy, B. R., & Maddireddy, B. R. (2022). AI-Based Phishing Detection Techniques: A Comparative Analysis of Model Performance. *Unique Endeavour in Business & Social Sciences, 1*(2), 63-77.

[32] Mithra Raj, M., & Arul Jothi, J. A. (2022, October). Website phishing detection using machine learning classification algorithms. In International Conference on Applied Informatics (pp. 219-233). *Cham: Springer International Publishing.* http://dx.doi.org/10.1007/978-3-031-19647-8_16

[33] Nirmal, K., Janet, B., & Kumar, R. (2021). Analysing and eliminating phishing threats in IoT, network and other Web applications using iterative intersection. *Peer-to-Peer Networking and Applications, 14,* 2327-2339.

[34] Rishikesh, Rupasri, Tamilselvan, Yoganarasimman, & Sujai, S. (2022). Intrusion of Attacks in Puppet and Zombie Attacking and Defence Model Using BW-DDOS. *International Academic Journal of Innovative Research, 9*(1), 13–19. https://doi.org/10.9756/IAJIR/V9I1/IAJIR0903

[35] Saha, I., Sarma, D., Chakma, R. J., Alam, M. N., Sultana, A., & Hossain, S.. Phishing Attacks Detection using Deep Learning Approach. *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT). IEEE.* http://dx.doi.org/10.1109/ICSSIT48917.2020.9214132

[36] Seyedan, A., Soroushpour, S., & Gholamrezazadeh, S. (2023). Family and its changes in Cyberspace and the explanation of its future perspectives in the communication era. *International Academic Journal of Organizational Behavior and Human Resource Management, 2*(2), 01–06.

[37] Sountharrajan, S., Nivashini, M., Shandilya, S.K., Suganya, E., Banu, A. B., & Karthiga, M. (2020). Dynamic Recognition of Phishing URLs Using Deep Learning Techniques. Advances in Cyber Security Analytics and Decision Systems. *Springer.* http://dx.doi.org/10.1007/978-3-030-19353-9_3

[38] Sree, K. S., Karthik, J., Niharika, C., Srinivas, P. V. V. S., Ravinder, N., & Prasad, C. (2021, November). Optimised conversion of categorical and numerical features in machine learning models. *In 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 294-299).* IEEE. https://doi.org/10.1109/I-SMAC52330.2021.9640967

[39] Subasi, A., & Kremic, E. (2020). Comparison of Adaboost with MultiBoosting for Phishing Website Detection. *Procedia Comput. Sci., 168,* 272–278. https://doi.org/https://doi.org/10.1016/j.procs.2020.02.251

[40] Subasi, A., Molah, E., Almkallawi, F., & Chaudhery, T. J. Intelligent phishing website detection using random forest classifier. *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA). IEEE.* http://dx.doi.org/10.1109/ICECTA.2017.8252051
[41] Taha, A. (2021). Intelligent ensemble learning approach for phishing website detection based on weighted soft voting. *Mathematics, 9*(21), 2799. https://doi.org/10.3390/math9212799
[42] Web page Phishing Detection Dataset. (2024, July 26). Retrieved from https://www.kaggle.com/datasets/shashwatwork/web-page-phishing-detection-dataset/data.
[43] Yang, R., Zheng, K., Wu, B., Wu, C., & Wang, X. (2021). Phishing website detection based on deep convolutional neural network and random forest ensemble learning. *Sensors, 21*(24), 8281. https://doi.org/10.3390/s21248281
[44] Zamir, A., Khan, H. U., Iqbal, T., Yousaf, N., Aslam, F., Anjum, A., & Hamdani, M. (2020). Phishing website detection using diverse machine learning algorithms. *The Electronic Library, 38*(1), 65-80. http://dx.doi.org/10.1108/EL-05-2019-0118

Author Biography

Sajidah Shahadha Mahmood received the B.SC. Degree in Control and Systems Engineering\Control Engineering in 2002 from the University of Technology in Baghdad, Iraq and M.SC. Degree in Control and Systems Engineering\Computer Engineering in 2020 from the University of Technology in Baghdad, Iraq. She is now a lecturer in the Department of Radio and Television Journalism, College of Mass Media, University of Al Iraqia, Baghdad, Iraq.