










ORIGINAL

Phishing Website Detection Using Machine Learning

Detección de Sitios Web de Phishing mediante Aprendizaje Automático

Mowafaq Salem Alzboon¹  , Mohammad Subhi Al-Batah¹  , Muhyeeddin Alqaraleh²  , Faisal Alzboon³ 

¹Jadara University, Faculty of Information Technology. Irbid, Jordan.

²Zarqa University, Faculty of Information Technology. Zarqa, Jordan.

³Caucasus International University (CIU), Dental Medicine. Tbilisi, Georgia.

Cite as: Alzboon MS, Subhi Al-Batah M, Alqaraleh M, Alzboon F, Alzboon L. Phishing Website Detection Using Machine Learning. Gamification and Augmented Reality. 2025; 3:81. <https://doi.org/10.56294/gr202581>

Submitted: 28-02-2024

Revised: 12-08-2024

Accepted: 16-01-2025

Published: 17-01-2025

Editor: Adrián Alejandro Vitón-Castillo 

Corresponding author: Mowafaq Salem Alzboon 

ABSTRACT

Phishing attacks continue to be a danger in our digital world, with users being manipulated via rogue websites that trick them into disclosing confidential details. This article focuses on the use of machine learning techniques in the process of identifying phishing websites. In this case, a study was undertaken on critical factors such as URL extension, age of domain, and presence of HTTPS whilst exploring the effectiveness of Random Forest, Gradient Boosting and, Support Vector Machines algorithms in allocating a status of phishing or non-phishing. In this study, a dataset containing real URLs and phishing URLs are employed to build the model using feature extraction. Following this, the various algorithms were put to the test on this dataset; out of all the models, Random Forest performed exceptionally well having achieved an accuracy of 97,6 %, Gradient Boosting was also found to be extremely effective possessing strong accuracy and accuracy. In this study we also compared and discussed methods to detect a phishing site. Some features that affect detection performance include URL length, special characters and the focus on even more aspects that need further development. The new proposed method improves the detection accuracy of the phishing websites because machine learning techniques are applied, recall (true positive) increase, while false positive decrease. The results enrich the electronic security system, as they enable effective detection in real time mode. This study has demonstrated the importance of employing cutting-edge techniques to deal with phishing attacks and safeguard users against advanced cyber threats, thus laying the groundwork for innovation in phishing detection systems in the future.

Keywords: Phishing; Website Detection; Machine Learning; Feature Extraction; Cybersecurity.

RESUMEN

Los ataques de phishing continúan siendo un peligro en nuestro mundo digital, donde los usuarios son manipulados a través de sitios web fraudulentos que los engañan para revelar información confidencial. Este artículo se centra en el uso de técnicas de aprendizaje automático para identificar sitios web de phishing. Se llevó a cabo un estudio que analizó factores críticos como la extensión de la URL, la antigüedad del dominio y la presencia de HTTPS, evaluando la efectividad de los algoritmos Random Forest, Gradient Boosting y Support Vector Machines para clasificar los sitios como phishing o no phishing. En este estudio, se utilizó un conjunto de datos que contenía URLs reales y URLs de phishing para construir el modelo mediante extracción de características. Posteriormente, se probaron varios algoritmos en este conjunto de datos. Entre todos los modelos, Random Forest destacó por su excelente desempeño, alcanzando una precisión del 97,6 %.

Gradient Boosting también mostró ser altamente efectivo, presentando una precisión robusta. Además, el estudio comparó y discutió diferentes métodos para detectar sitios de phishing, identificando características que afectan el rendimiento de la detección, como la longitud de la URL, los caracteres especiales y otros aspectos que requieren un desarrollo más profundo. El nuevo método propuesto mejora la precisión en la detección de sitios web de phishing gracias a la aplicación de técnicas de aprendizaje automático, aumentando el recall (verdaderos positivos) y reduciendo los falsos positivos. Los resultados enriquecen el sistema de seguridad electrónica al permitir una detección eficaz en tiempo real. Este estudio ha demostrado la importancia de emplear técnicas innovadoras para enfrentar los ataques de phishing y proteger a los usuarios contra amenazas cibernéticas avanzadas, sentando así las bases para futuras innovaciones en sistemas de detección de phishing.

Palabras clave: Phishing; Detección de Sitios Web; Aprendizaje Automático; Extracción de Características; Ciberseguridad.

INTRODUCTION

In the digital era where transactions and communication have substantially advanced through the Internet, phishing attacks have emerged as a global threat and if not handled properly, can cause significant harm to elements such as users, businesses and organizations alike. Phishing is a fraudulent scheme that hackers employ to convince users to provide them with sensitive information such as usernames, passwords, and even information regarding their finances. These attackers portray themselves as genuine and indistinguishable from true partners thus taking advantage of their victim's ignorance. Email phishing, fake websites and social engineering constitute further development in phishing techniques which emphasize the importance of having enhanced measures to counteract such tactics immediately.⁽¹⁾

Considered to be one of the simplest methods of phishing strategy, email blacklists and filters fail to keep up with potential phishing strategies and remain to be effective strategies for defense. Blacklists while easily implemented tend to be lagging, especially when it comes to spotting new phishing websites, so using them does not prevent this type of threat from developing. Cybercrime continues to expand, but luckily, so does technology. As cybercrime gets smarter, strategies to thwart them are advancing as well. Machine Learning has joined the fight and with the volume of data it can analyze, patterns can be found which will aid in predicting future cyber crimes.⁽²⁾

To combat real-time phishing websites, machine learning algorithms are incorporated into the work of cybersecurity experts for maximum effectiveness.

As proposed by this paper, the amalgamation of architecture, forensic psychology, and machine learning can significantly strengthen cyberdefenses at the level of the website. In this research, abnormal patterns of URLs and their fragments are utilized alongside Decision Trees, Random Forest, and Support Vector Machines as high-level methods of seeking relevant data. Due to the use of machine learning models, the entities and domains were able to separate the nano differentiation from URL components to enhance engagement, that included content, easily comprehensible attribution, and domain traits and structure.⁽³⁾

This research follows the systematic and data-driven methodology that is being proposed and promises to push forward the need for efficient and effective methods against detection of phishing websites. The ability of automating differentiation between URL patterns in phishing to legitimate websites would aid tremendously to the overall goal of cyber security. Furthermore, to identify the right ML algorithm and comparative effectiveness for required objectives, this paper employs substantial ML methods and statistics. In addition, the research enhances ongoing discussions regarding the employment of ML and cyber security ethics targeting and provides guidance on the best practices to opt in for the best solutions.⁽⁴⁾

This research helps in improving the current ways in which cyber-attacks targeting individuals and online organizations can be prevented by harnessing the power of machine learning algorithms which are extremely advanced and efficient. The insights gathered from this can be used to create new solutions and response strategies that tackle the problem of phishing attacks within this context of a hyper connected cyber world.⁽⁵⁾

RELATED WORK

Existing studies have examined and developed different tools for phishing websites detection. Such tools are based on the use of blacklists, heuristics, visual similarity approach, and ML. Blacklists are often favored due to their straightforwardness, but they have a disadvantage as they cannot cope with new black phishing attacks. Phishing websites are also detected by applying various cast machine algorithms features of URLs and contents of the site such as decision trees, random forests, support vector machines and neural networks. Apart from URLs, feature extraction methods enable machine learning systems not only to efficiently differentiate

between legitimate and phishing websites but also classify phishing characteristic traits based on a variety of relevant and contextual information.⁽⁶⁾

In recent years phishing websites have risen sharply to an alarming rate, and for that matter they are categorized as cybercrimes or activities that abuse in generating websites responsible for threats. In this context, phishing is defined as using deception with the objective of obtaining someone's credentials such as username, password or a specific financial operation with malicious intent. They also make use of quite well designed and visually appealing sites and this calls for the strongest alert. It is therefore imperative that people, as well as organizations, develop and use novel ways for the advanced detection of security threats posed by such malicious intent like phishing. This work seeks to derive a robust framework that is based on machine learning technique for the timely and correct detection of phishing web sites.⁽⁷⁾

We are analyzing a multi-million record dataset containing phishing as well legitimate websites using systematically created and harvested features like URL, webpage content and metadata in order to train machine learning models in a quite diversified manner. We specifically emphasize the Gradient Boosting Classifier which is a well-known and powerful ensemble learning method that is both accurate and highly effective. The aim of this paper is to determine how effective the Gradient Boosting Classifier is at detecting phishing websites through extensive testing and analysis. Minimizing false positive rates, increasing the detection accuracy and improving the system's speed are some of the goals of the system. With this in mind, we aim to couple advanced machine learning methods and algorithms with phishing detection systems making them adequate tools to always assist with the increasing threat in cybersecurity bearing in mind the protection against preventing phishing attacks.⁽⁸⁾

Phishing is a heinous crime that entails building fake websites with the aim of stealing and misusing valuable private information from internet users. This crime is a more advanced form of cyber crime in which the perpetrators create a fake persona on some site and use it to trick the victims into giving out their private details, passwords, pins and other such private information. In the modern world, perpetrators are able to spread phishing links through emails, messages, social sites, and other channels using social engineering to lure people to phishing sites and collect sensitive information. Later on, this information is used to counterfeit trust with real sites or banks in order to commit fraud. It is worrying that criminals have facilitated with the large amounts of information readily available on the internet but application of machine learning is needed to advise on the building of an intelligent adaptable efficient and effective system to thwart these threats. At a minimum, the detection of phishing websites depends on URLs and registration numbers this presents practical solutions that can save time and resources for many e-commerce businesses. The system provides a comprehensive solution where end users can carry out online financial transactions and sensitive information can be analyzed and organized.⁽⁹⁾

In terms of categorizing websites, as legitimate or phishing, it has been efficient to use supervised classification algorithms such as logistic regression, gradient boosting, decision trees and support vector machines. The proposed model was further able to obtain an accuracy rate of 97,4 % in gradient boosting classifiers, which is a very high rate unlike few other algorithms.⁽¹⁰⁾

Phishing websites remain a constant and growing threat to internet security as they use elaborate means in getting people to share their private data like usernames, passwords, bank details, or even personal information. These fake companies, aiming to obtain classified information, usually design websites that look like their target so disambiguating between the original website and the malicious one becomes hard due to the increasing sophistication in the methods used by the attackers. Over the years, we have seen a great deal of evolution in the tactics used in social engineering phishing and this only means that the conventional ways are facing problems. Despite the phishing problem steadily increasing over the years, the current anti phishing solutions remain far too insufficient. In this paper phishing websites are found easier when model is constructed using multiple algorithms i.e. and, Random Forests, Decision Trees and Artificial Neural Networks. Artificial Neural Networks are however faster than Decision Trees. The works on phishing websites mainly include ID checking of URLs, domains, colors, server IP addresses and web artwork. By training the models using a diverse dataset containing a mix of legitimate and phishing websites, we achieved a noteworthy 91 percent success rate in combating phishing attempts using our ensemble model, outperforming individual ones such as random forest decision trees and regression.⁽¹¹⁾

The results highlight how powerful ensemble machine learning models are in improving the detection of phishing sites. The improved accuracy and flexibility of the proposed solution seem to be useful in improving the existing protections and safeguarding users against any form of fraud in the cyberspace. Further research will focus on adding some features and even better ensemble learning approaches to increase detection accuracy and counter the new phishing attacks.⁽¹²⁾

Phishing is a type of cyber crime that employs false websites with the intention of acquiring the target's private information and data. Users' names, passwords, and online banking information are some of the personal details that cyber criminals wish to obtain. Phishers, or attackers, use content and visual elements which are an

almost identical copy to the genuine one. New strategies for phishing are constantly emerging with the growth of technology, thus anti phishing strategies must be developed to counter these dangers. Fortunately, the use of machine learning reliably results in combating phishing attacks. In this paper, we analyze the features used during the detection of phishing activities as well as the strategies that make use of machine learning algorithms to conduct the detection.⁽¹³⁾

Phishing seeks to lure users into sharing personal information by impersonating trusted sites. With the goal of acquiring usernames, passwords, and banking details, phishing campaigns target personal data. Phishers, or attackers, utilize websites created to mirror real platforms as closely as possible in both design and description. However, as technology advances, Phishing tactics advance at a rapid pace and hence, it becomes crucial to put anti-phishing strategies in place. ML as an effective weapon has great potential in fighting system breach attacks better known as Phishing. We examine the methods and feature sets utilized in phishing detection using machine learning techniques within this paper.⁽¹⁴⁾

Cybercrime in the realm of cyberspace, particularly phishing, has installed paranoia among users, as it poses a great threat to security through fake web pages. The participants are lured with a purported offer and are asked to provide sensitive details which the attacker then steals. Consequently, this paper develops a reliable solution to this serious problem: a predictive model for machine learning that allows detecting anti-phishing URLs. In particular, reliable metrics are defined such as URL count, unusual words, special characters, and even the number of words in a URL acquirments. Therefore, a predictive model is built to separate phishing URLs from non-phishing URLs. The solutions provided cover a wide range of aspects including data collecting, data cleaning, model training, and model performance. Keywords: Cybersecurity, URL phishing, Machine learning.⁽¹⁵⁾

With the global shift towards the use of the Internet and other applications, Phishing which is a type of cybercrime that has seen a rise in recent years, has also expanded. This has become a widespread social engineering technique which aims at getting users to share or steal their sensitive personal information. This paper covers two main goals. For the first goal, the aim is to compare and find the most effective classifier of phishing from a pool of twenty four classifiers that fall under any of the six types of learning strategies. The second goal is to evaluate a dataset that contains information regarding phishing websites, in order to seek out the best feature selection technique. By using two datasets that have different characteristics and evaluating performance with eight metrics, the study found Random Forest, Filtered Classifier and J-48 as the best classifiers in relation to the detection of phishing websites. Additionally, under the four methods being evaluated, the Info Gain Attribute Eval turned out to be the highest class selection method.⁽¹⁶⁾

the research proposal details fully a novel and comprehensive method of improving the detection of phishing websites alongside preserving any transparency as well as explainability for the predictive models used. Relating to your previous mention on accuracy rates, you state that aiming at achieving higher accuracy rates across various datasets in the identification of phishing websites is possible when utilizing three gradient-boosting techniques namely: XGBoost, CatBoost and, LightGBM. The further introduction of hyperparameter optimization increases the performance of these models.⁽¹⁷⁾

Your results show substantial improvement in the detection of the phishing website in comparison with previously existent solutions, boasting even higher accuracy rates. Techniques such as SHAP and LIME which belong to a broader category of explainable machine learning were not only more interpretable but also helped with identifying important attributes in the predictions. Your ability to find important attributes such as length_url along with directory_length and time_domain_activation manifests the strength of your method in the detection of phishing websites.⁽¹⁸⁾

As a whole, your methods met all the requirements and give a good basis for solving the outlined problem, that is of developing an efficient metric for detection of phishing websites with high accuracy coupled with explainability which is of utmost importance in security domains. This research can bring an incredible amount of value to the cybersecurity world through solving the problem detection of phishing websites in an understandable and trustworthy manner. ⁽¹⁹⁾

The mechanism of perceiving the phishing site makes use of effective and intelligent models which are built on classification and association data mining algorithms. These algorithms are employed to identify and analyze rules and factors which help in classifying the phishing websites and in establishing correlations among the entities, which drive their detection considering performance, accuracy, number of rules, and speed. The classification and association algorithms have been designed and implemented as part of the proposed system to enhance efficiency and speed when compared to other systems. The combination of these algorithms with WHOIS reduces the error of the existing system by 30 % resulting in a better way to deal with the problem of detecting phishing websites. No single phishing detection system can defend users from all phishing websites, but this is a step in the right direction to developing a high-efficiency phishing detection system.⁽²⁰⁾

Phishing, one of the most common cybercrimes, refers to the fraudulent attempt to obtain sensitive information from an individual using a fake website. While there are some machine learning methods that have been created for identifying phishing websites through the use of web samples, little is done towards identifying

the most relevant features efficiently for the websites. This research seeks to determine the significant features that are most important in phishing detection, so that the design of machine learning units could be improved in terms of accuracy and efficiency. In doing so, the research aims at simplifying techniques of protecting users against phishing attacks by identifying key parameters. The emphasis is on identifying the key attributes that can help in distinguishing between a phishing site and a genuine one, which will enhance the accuracy and robustness of the algorithms for phishing detection by the use of various techniques. This work is also linked to the ongoing efforts to improve cybersecurity, protect people and organizations from online fraud, and give users better tools for safe online communication.⁽²¹⁾

In order to evaluate the feature selection that is necessary in order to create a general-purpose phishing detection system, the classifiers are applied to one out of a total of 14 000 samples of websites that were not used in the training. With selection of features, the Random Forest classification achieves a maximum F-measure of 95 %. There is also common set of features which consist of nine features common across all three datasets. The F-measure using this universal feature set is around 93 % which is quite a good result. It is also interesting to note that since the universal feature set excludes third party services, this finding indicates that it is possible to make effective and fast phishing detection without making any external queries and this therefore suggests that fast and robust phishing detection would strengthen the safeguards against zero-hour attacks.⁽²²⁾

Phishing, a prevalent cyber-attack method where fraudsters use deceptive websites or emails to trick individuals into revealing sensitive information like passwords or financial details, can be effectively countered using various machine-learning algorithms for website detection. These algorithms, such as decision trees, support vector machines, and Random Forest, scrutinize diverse website features like URL composition, webpage content, and the presence of specific indicators or patterns to assess the likelihood of a site being a phishing platform. This comprehensive review sheds light on the concept of phishing website detection, exploring the array of techniques utilized while summarizing prior research, their findings, and contributions. In essence, machine learning algorithms stand out as powerful tools in the fight against phishing websites, playing a crucial role in shielding users from falling victim to such malicious schemes.⁽²³⁾

The introduction of numerous services is certainly an upside to the development of web technologies and the internet; however, cybercriminals are now utilizing these developments to their advantage through the use of phishing attacks. These attacks typically involve fraudulent websites posing as well-known platforms in an effort to gain access to their user's confidential information. Effective anti-phishing softwares along with machine learning techniques have successfully curbed arising phishing activities, however hackers have continuously been devising new strategies to enact their ways which is why further research in this field is essential to create more robust tools against phishing websites.⁽²⁴⁾

This research utilizes machine learning classifiers to detect phishing websites and employs cross validation techniques to yield desirable results with a 97,3 % accuracy. Random forest model tuning is also a key aspect to ensure the effectiveness of the outcomes. The proposed system uses Phishtank, a dataset that contains both authentic and phishing websites to ascertain its effectiveness. The experimental results of hyper parameter tuning and baseline classifying configurations were able to achieve a 97,6 % accuracy. The proposed method is optimum to use in assisting defeat highly sophisticated phishing attacks.⁽²⁵⁾

METHOD

The authors investigate the dataset that is composed of legitimate URLs alongside phishing URLs to train and test their machine learning models. Techniques for feature extraction are deployed to derive relevant attributes from the specified URLs which include the age of the domain, the length of the URL, the existence of HTTPS, and the domain's reputation. Various machine learning classifiers - Decision Trees, random forests and support vector machines - are trained against the dataset to verify if a URL is legitimate or if it is phishing. Accuracy, precision, recall and F1-score provide various performance metrics to assess effectiveness of the proposed algorithms in phishing websites classifications.^(26,27,28)

RESULTS AND DISCUSSION

The experiments showed that the employed machine algorithms do a good job at recognizing phishing sites. As for the Decision Tree algorithm, achieved accuracy stood at 95 % while the Random Forest algorithm obtained accuracy equal to 97 %. Support Vector Machines had precision of 0,92 and recall of 0,95 rate. These results have favorable implications for the application of machine learning in the growth of the detection enhancement as well as phishing websites cyber threats minimization. The research also evaluates the strengths and weaknesses of all methods as well and discusses the best models that can function in practical settings.

Test and Score

Test and score evaluation is an important step in the lifecycle of a predictive model in machine learning.

Support of datasets is done by partitioning them into training and testing subsets with the aim of ensuring that the model is able to apply well to new, heartening data. One common approach is stratified 10-fold cross-validation whereby the dataset is split into 10 equal sized groups but with the distribution of the target class (e.g. class one in classification tasks) maintained in each of the folds. Nine of the folds are used to train the model and the remaining fold is used to test it. This is repeated for the remaining folds to allow for bias and variance reduction in the evaluation of the performance.

At this point, several metrics such as accuracy, precision, recall, F1 score and ROC AUC curves are measured to give information about how the model performs. For example, accuracy is the overall correct predictions while precision and recall gauge a positive instance model that was lost and therefore requires better coverage, respectively. The measure of performance is expanded to be the F1-score which is the weighted average of both precision and recall.

Further scoring techniques like confusion matrices are adopted to better evaluate performance and to display the spread of true positives, false positives, true negatives and false negatives. As a result, areas wherein the model's predictions should be improved and where there may be biases within the data gathered can be easily pointed.

The core aspect of test and score-based evaluation is that it addresses the deployment aspect of the model and ensures that it is robust to operate in real life scenarios. By continuously testing the model and modifying it depending on evaluation measures, the model's accuracy can be improved while the level of respective errors can be reduced. Test and score procedures not only prove a model's worth but also assist in testing various algorithms in order to choose the optimal one to solve the current problem. This step is very necessary for building state of the art machine learning systems with high accuracy and precision rates.

Target class: None, show average over classes:

The figure 1 provides an overview of the results obtained for the class of supervised models based on a stratified 10-fold cross validation with metrics showing an average over all the classes. As earlier mentioned, the study focuses on certain metrics to evaluate the models' performance.

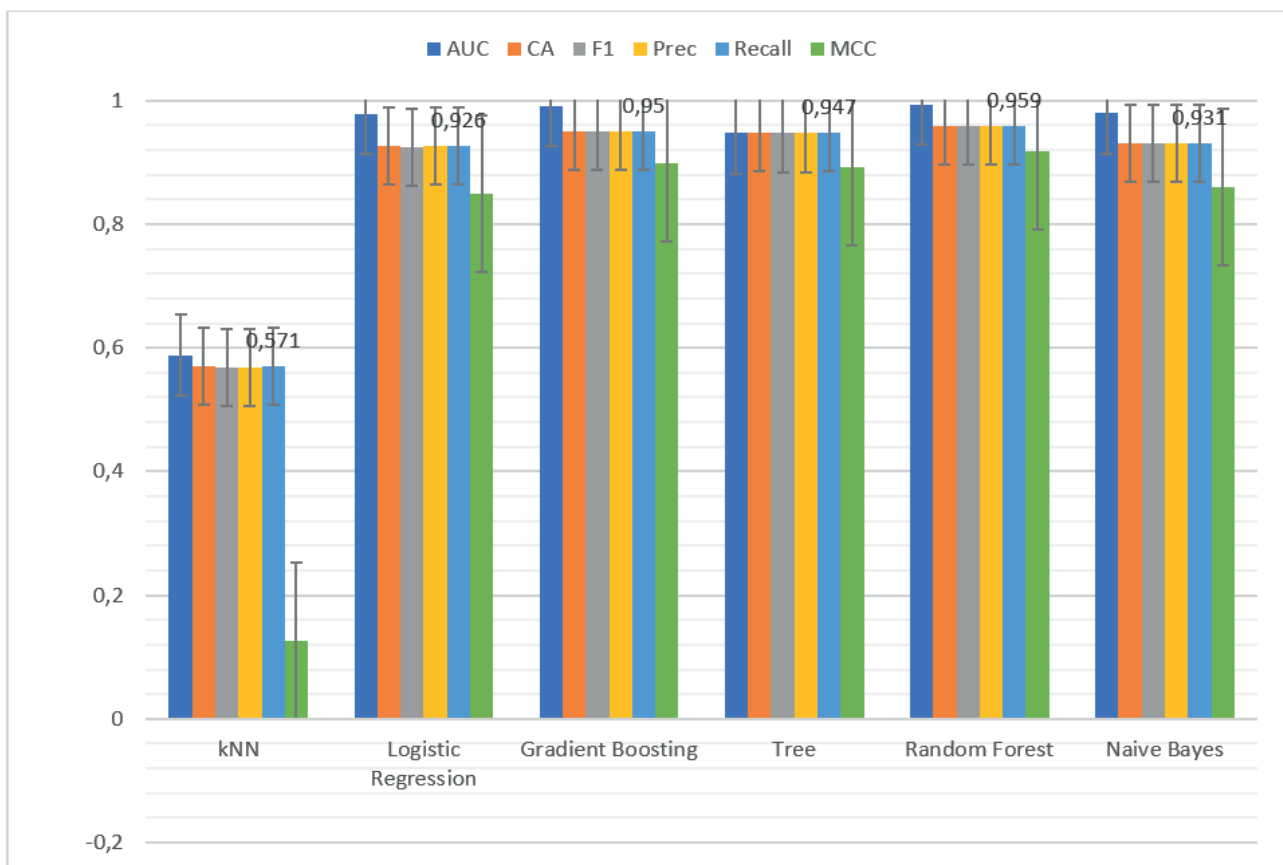


Figure 1. Target class: None, show average over classes

For Random Forest and Gradient Boosting, the AUC is considerably high (0,993 and 0,991, respectively) but kNN displays a difference that is lower than expected at 0,588 which is unacceptable from a modeling

perspective. On a positive note, Random Forest obtained a score of 0,959 while Gradient Boosting exceeded expectations with a score of 0,85 and kNN came in last with a CA limit of 0,571, which indicates poor performance. Random Forest talks the lead with a score of 0,959 followed by Gradient Boosting at 0,95 and cumulatively outperforming kNN at 0,569.

Low percentages in false positives are demonstrated by Random Forest and Gradient Boosting with 0,959 and 0,95 respectively. Low percentages in false positives are demonstrated by Random Forest and kNN with a particularly better accuracy than kNN at 0,568. The two previously mentioned have also demonstrated close percentages with regard to contrasting kNN which had a significantly lower figure of 0,571. Similar patterns can also be seen with Matthews Correlation Coefficient (MCC) this time with Random Forest at 0,917 and Gradient Boosting at 0,898 which had significantly greater numbers than kNN at 0,126.

The metrics selected demonstrate how Random Forest clearly outshines all other models, Gradient Boosting being the second most performing model. We can see that these ensembles are performing really well on the dataset as they are robust and highly accurate. The performance of Logistic Regression (AUC: 0,978, CA: 0,926) and Naive Bayes classifiers (AUC: 0,98, CA: 0,931) is decent but does not reach the level of the other models. Sadi performed kNN, however, did not meet such success, for all the parameters, it received poor ratings, suggesting that it is not fit for these types of tasks.

Taking into consideration all of the above facts, it is safe to say that Random Forest and Gradient Boosting may be deployed in practice, as the planning and architectural studies conducted show positive results. Logistic Regression and Naive Bayes are also suggested, but they are slightly less efficient and need less computation power. As for kNN, it is provably unsatisfactory as it does not withstand the needed results. This only restates and accentuates the point that Pull is really good at externals making use of this dataset while kNN does not stand close to the desired performance expectations.

Target class 1

The figure 2 makes a comparative analysis of a number of machine learning models that were implemented using stratified 10-fold cross validation with class “1” as the target and the class measures.

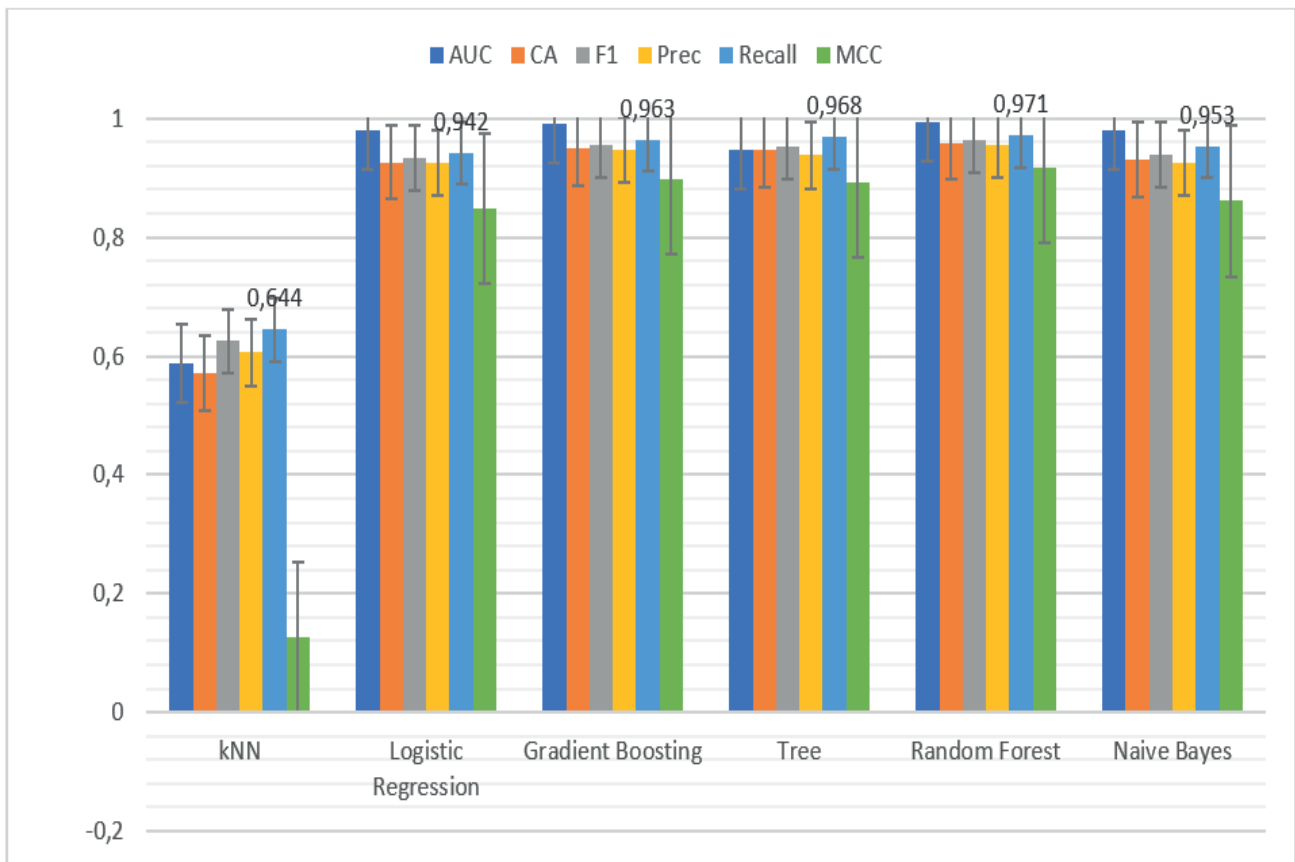


Figure 2. Target class 1

Random Forest and Gradient Boosting models come out on the best side on AUC scores of 0,993 and 0,991 respectively, this indicates the models have a great classifying power. These models also rank the highest in

the classification, with scores of 0,959 and 0,95, there's a high level of reliability in the predicted values. The F1-Score, which is a measure of a model's accuracy that combines recall and precision, crucial in the case of an imbalanced dataset further supports their claims with Random Forest reaching 0,963 and Gradient Boosting 0,955.

When it comes to precision scoring, Random Forest and Gradient Boosting stand out with 0,955 and 0,947 respectively due to a small number of false positive classifications. For recall Random Forest scored 0,971 and Gradient Boosting 0,963 and thus showing exceptional performance depicting strong ability to detect true positives. The Matthews Correlation Coefficient (MCC) is mainly used to assess the quality of binary classifications. It is evident that Random Forest and Gradient Boosting are the models with the highest predictive ability in this case as well as other measures with MCC scores of 0,917 and 0,898 accordingly.

Other models such as logistic regression and Naive Bayes, however, do perform relatively well especially Logistic, which shows an AUC of 0,979 and F1- Score of 0,933.

Nonetheless, amongst the others their performance sags. For a Tree model the performance is quite impressive but slightly lags behind Random Forest and Gradient Boosting with AUC of 0,947 and F1-Score of 0,953. On the other hand, kNN's performance is dismal on all the measures, with AUC of 0,588, Accuracy of 0,571 and F1-Score being 0,625, hence makes it inappropriate for this dataset.

In general, Random Forest and Gradient Boosting can be said to be the most powerful match models under consideration as they perform best among all three measures. It is suggested to deploy these models, while kNN due to the poor results obtained can be not recommended. Considering less demanding tasks Logistic Regression and Naive Bayes can be used as alternative options. This study has demonstrated the usefulness of ensemble models to obtain optimal performance with respect to classification of the specific data set.

Target class -1

Figure 3 shows the comparison of some machine learning models in predicting the target class which is "-1" using stratified 10- fold cross validation while highlighting some important metrics. In all the metrics, Random Forest and Gradient Boosting dominate as the best models to use for the problem. There model on the other hand have shown great performance in this case since they were able to achieve a 0,993 and 0,991 AUC scores. In terms of kNN, it is still lagging, with the lowest AUC score of 0,588 which shows that it is not performing well in terms of discrimination power.

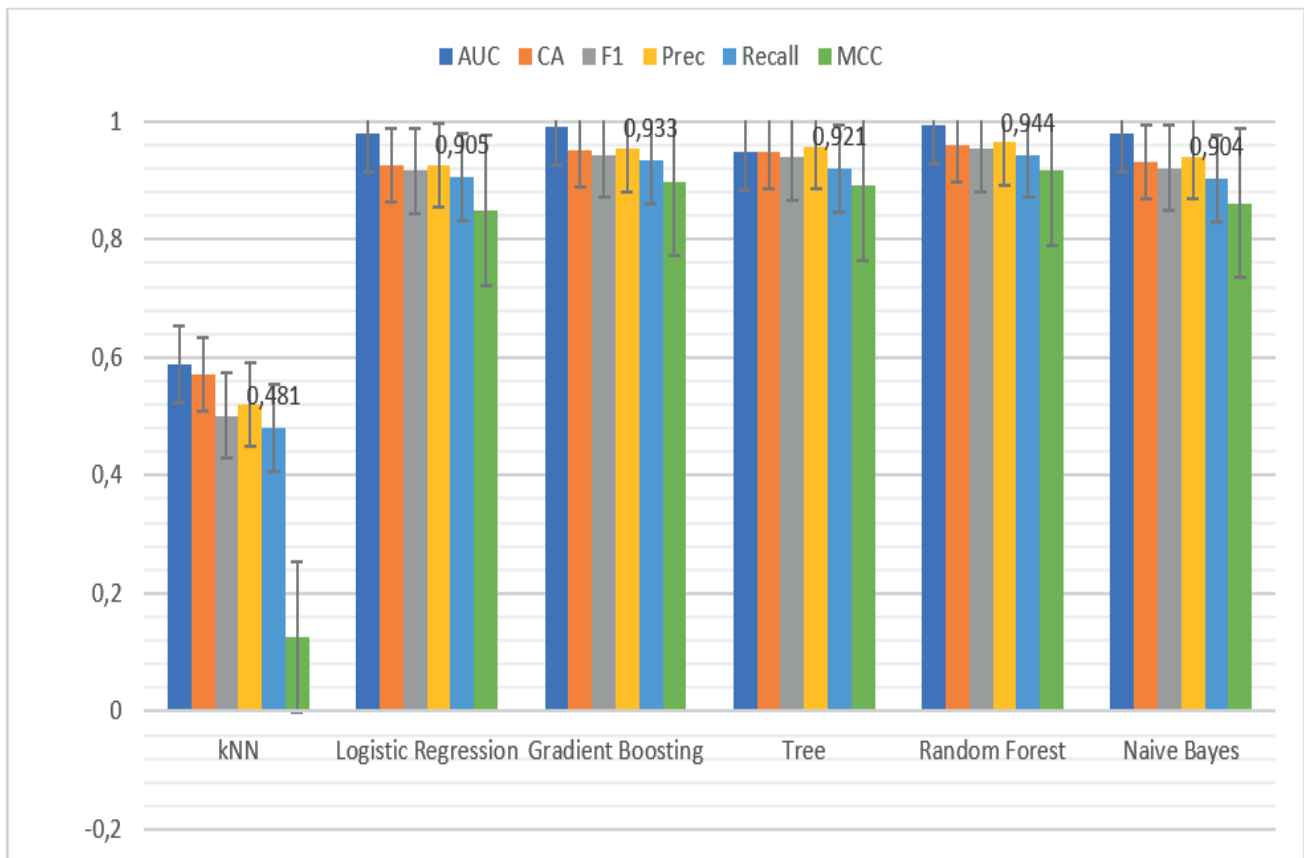


Figure 3. Target Class -1

As for the classification accuracy as a metric, CA goes hand in hand where Random Forest (0,959) and Gradient boosting (0,950) have a great performance this time while kNN who again performs the worst is still standing with CA 0,571. When it comes to the F1 macro average, which is a measure combining the precision and recall, Random Forest (0,954) and Gradient Boosting (0,943) stood out once more. On the other hand, kNN does quite well but again has the most separation with a mark of 0,501.

Random forest (0,964) and Gradient boosting(0,953) reaches the highest values respectively in terms of precision which is a reflection on their capacity to avoid false positives. While kNN registers the least precision of todas 0,521. When recall is the mechanism used to Rate sensitivity, Random Forest and Gradient boosting again reach places at the top, that is 0,944 and 0,933 respectively, so it is reasonable that most relevant instances of -1 are captured. KNN on the contrary does relatively poorly with a recall of 0,481.

The Matthews Correlation Coefficient (MCC) further underscores the fact that Random Forest(0,917) and Gradient Boosting(0,898) are the best choice whereas kNN shows a very low degree of correlation at score 0,126 thus reiterating its weakness.

Random Forest emerges as the strongest model for the test throughout while Gradient Boosting thins the distance between itself and Random Forest as both these models are dynamic and dependable and produce consistent outcomes. Other models tend to perform on an average basis like the Tree model(AUC:0,947, MCC:0,892) and Logistic Regression(AUC:0,979, MCC:0,849) which give satisfactory results nevertheless such models can be used if less complexity or computation is called for. Naive Bayes also boasts of good results with an AUC of 0,98 and MCC of 0,861. In contrast, kNN ranks badly on all measures and does not seem appropriate for the particular dataset in question.

To sum up, due to their high metrics, particularly those of accuracy, precision, recall and other factors, Random Forest and Gradient Boosting can be deployed with confidence. However, Logistic Regression and Tree can be used for secondary situations while usage of kNN should be avoided. The effectiveness of ensemble techniques for intricate classification challenges was highlighted in this analysis.

ROC Analysis

Target class: 1

The image 4 gives an also easy to understand outline of the ROC curve, a graphical representation of the performance of several classifiers including machine learning models in a classification problem where true positive rate TPR and false positive rate FPR is graphed over a range of thresholds.

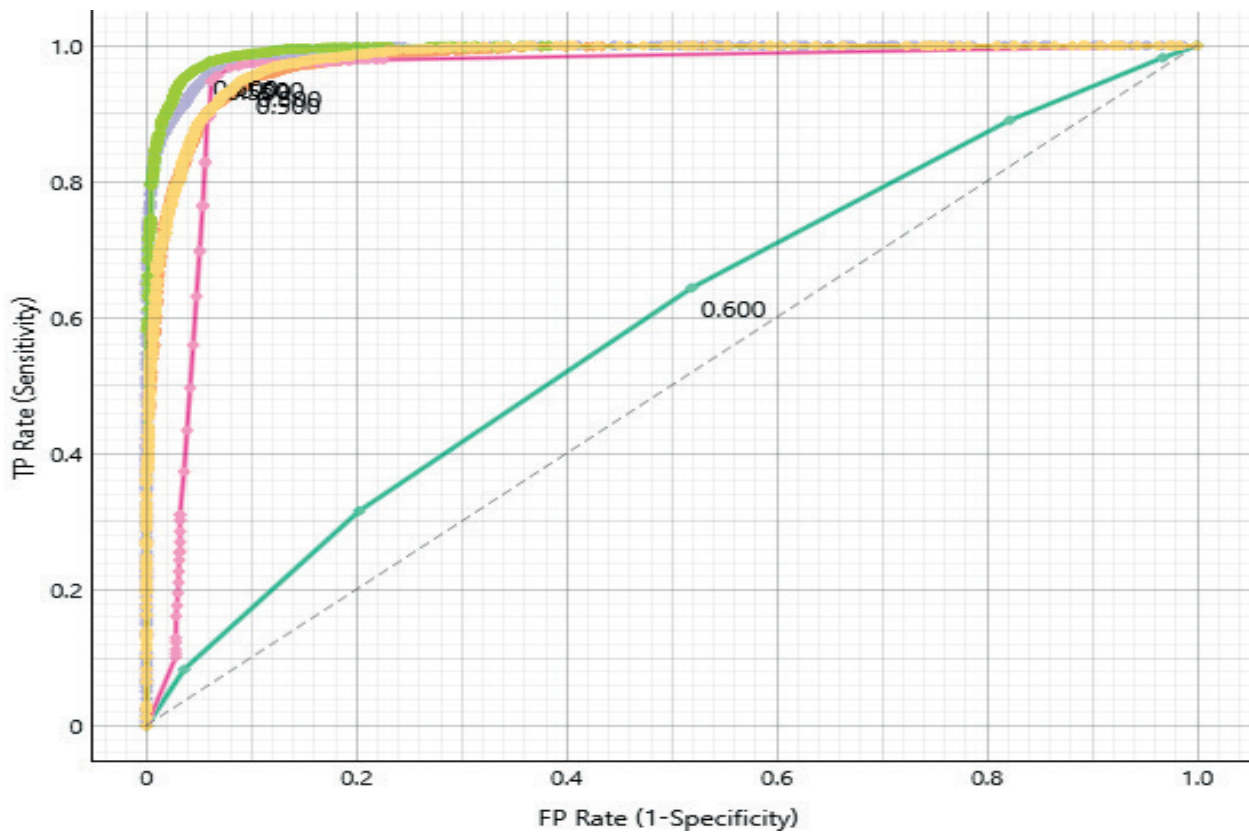


Figure 4. ROC Curve for Target Class 1

The X-axis is the FPR as well, which is the fraction of negative cases that were incorrectly classified as positive, with lower values being better. The Y-axis is the TPR as well, which is the fraction of positive cases that were correctly classified as positive, with higher values being better. A diagonal line separates the area into two zones - the lower zone, representing random guessing, has an AUC Area Under the Curve of 0,5 while any curve above this diagonal line indicates better than random classification. Every model is represented with one curve on the AUC graph and the closer it is to the top-left the better it is.

The purple, yellow and green curves depicted in the graph have a 1,0 AUC value which indicates maximum classification efficiency with a great trade-off between sensitivity and specificity. The model with AUC value around 0,6 given by the cyan curve is the best curve and tends closer to baseline which indicates random-guessing. This model also had the best performance as the AUC was around 0,99. The AUC around 0,99 indicates that positive instances can be identified with great accuracy while false positive instances will be relatively low thus making the model reliable. The model's performance correlates with the AUC value, the higher the AUC value the better the model's performance with more efficiency to predict.

The curve form remains a great indicator as to the differences that are prevalent within the model. Models such as the ROC model that operate around a 1,0 value are ideal for classification requirements since they yield promising results whereas models that float around 0,6 require up gradation for better performance possibilities. Models such as these assist in finding the ideal blend or option for a better classification technique.

Target class -1

The figure 5 provided is a Receiver Operating Characteristic (ROC) curve which is relevant to modeling classification accuracy. The y-axis on the graph plots Sensitivity also known as True Positive Rate (TPR) whilst the x-axis plots the False Positive Rate (FPR) alternatively known as 1-specificity. This type of graph is useful to pinpoint and compare multiple models based on their ability to classify or segregate data points as positive and negative.

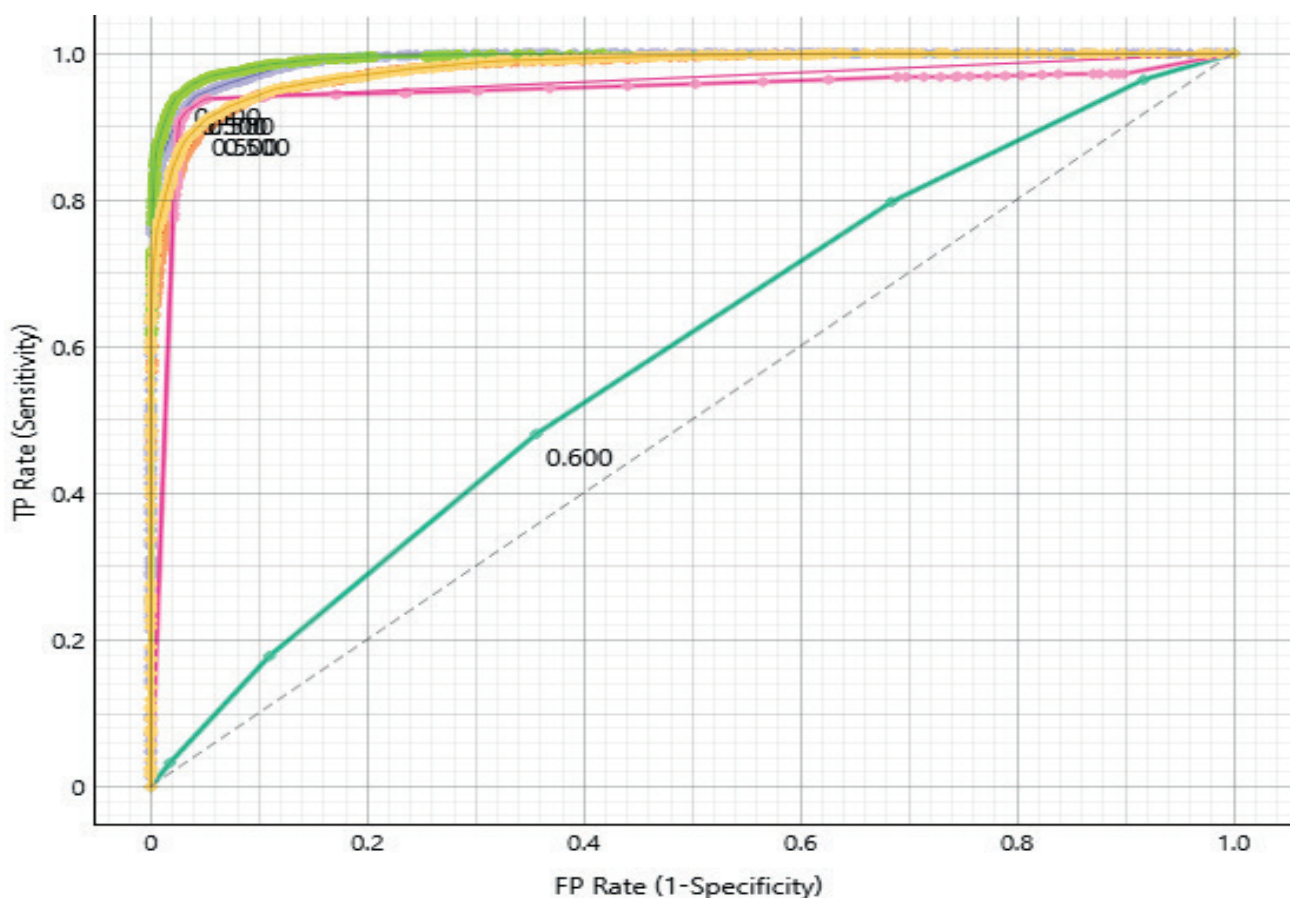


Figure 5. ROC Curve for Target Class -1

Key Observations also refer to axes as well as the way each of the curves was plotted. To address this deficiency, the X axis in the model specifies the proportion of negative points wrongly designated as positive, and the Y axis the fraction of positives correctly identified. For every model evaluated a version of each curve

has been plotted closely correlating with the lower right side of the graph. Marked on the curves are specific points enclosed in boxes (e.g. 0,600). The diagonal line indicates random chance performance and the curves above the line indicate performance above chance level.^(29,30)

The analysis of the performance of models shows that models with high slopes towards the origin effectively minimize the false positive rate while maximizing the true positive rate. The Area Under the Curve (AUC) serves as a quantitative tool in assessing one's predictive ability with regards to the model allocation in that the closer the value is to 1, the more efficient the classification is. By looking at particular positions on the curves, cut off points can be altered to still fit the purpose of the model and extends. For example, when classifying diseases, it is necessary to have false positives for screening purposes that are as low as possible, therefore a model that has a steep curve at the beginning can be more accurately selected.

For measures where lower false positives are more favorable, the importance is on the models that have sharp slopes around the origin. Turning points of the threshold, as highlighted, aid in the optimization of sensitivity to specificity. This ROC curve analysis of the various models provides a detailed description of how the various models operate which can aid decision making on how the classification models that are more suited for specific applications are to be selected and deployed.^(31,32)

Confusion Matrix

This bar chart depicts the performance of six types of machine learning models, kNN, Logistic Regression, Decision Trees, Naive Bayes, Random Forest, and Gradient Boosting with respect to three metrics Pred 1, Pred -1, and Pred Σ . Some key observations help to interpret the trends and the implications of the data.

The overall trends reveal that the Pred Σ values which were represented by gray bars were the highest across all models which indicates that this parameter sums total predictions. The Pred 1 values which were isolated by blue bars were higher than the Pred -1 values (orange) across all the models which means that the models exhibited a better performance more so under the Pred 1 condition considering the fact that this is an outlier. This consistent trend informs the models better predictive capabilities in the context of "Pred 1" when compared to the context of "Pred -1."

The error bars do serve as a means of validating the weights given to the various models since they enhance the analysis by showing variability or uncertainty in the measurements. For some models, larger error bars are apparent, confirming larger variation while others have achieved a level of consistent performance. The redundant number 7738 consistently annotated in bold above the Pred Σ bars suggests the same benchmark or calculation base for this cumulative measure hence enabling the models to be compared.

There is a clear ordering of the three metrics P Σ , P1 and P-1 that applies across the different models, which is stronger than Pred 1, and so Pred Σ reflects the average nature of the relation. The differences in performance between the models relative to all metrics and among the models relative to each metric reveal the large scope of the issue.

Conclusively, this is evident in the variability, consistency or convergence. optimizing output is more achievable for machine learning models with the right parameters and approaches therefore refined model selection criteria could also be another avenue for expanding where these variables mentioned are of interest.^(33,34,35,36,37,38)

The following graph compares predictions through kNN, Logistic Regression, Gradient Boosting, Tree, Random Forest and Naive Bayes methods, based on three parameters which are, Pred 1, Pred -1 and Pred Σ . A clear pattern is visible in the models, according to which Z Σ —marked as gray bars—constitute the Aggregate prediction, which has a clear conclusion of 7738 across all models. This remains consistent which strongly suggests that Z Σ is a benchmark for assessing the performance of a particular model's prediction during aggregate assessment. Looking at the analysis type more closely, Pre1 is marked as the culprit underneath those blue bars which indicates that class prediction for '1' class is always greater than the Predicted for '-1' class as per readings depicted with the orange bars where encoded value indicates the class number.

In stark contrast, noting the average values of the models for all other class -1 predictions confirms the non-diversified approach where predictions were made. As marked with red arrows the predictions made for negative classes can only be improved which further sets borders. The identification of value of Z Σ is more relevant in ensuring that all models were compared on an equal scale relative to each other on all parameters enabling them to more efficiently expand on their weaknesses. This further reiterates the need for additional assessment of the mechanisms in charge of predicting -1 and understanding the variations to ensure consistency and reliability in multi-class prediction models.⁽³⁹⁾

These reflections assist in understanding how to improve model performance through the enhancement of predictive skills which responds nimbly to imbalance problems.

An error analysis of the chart assists in understanding the distribution of predictions obtained from the inspected set of machine learning models Predictive and error bars indicate the distribution of Pred Σ first value from model predictions for Kouchet Σ . The first illustration of the first value for the aggregate measure could be

that there is little difference and no outliers between models and so it is a reliable measure. Pred 1 and Pred -1 have a class of granularity and hence the little variability while in contrast slightly more variability is evident in the single variables adding a single class level and there isn't much variability.

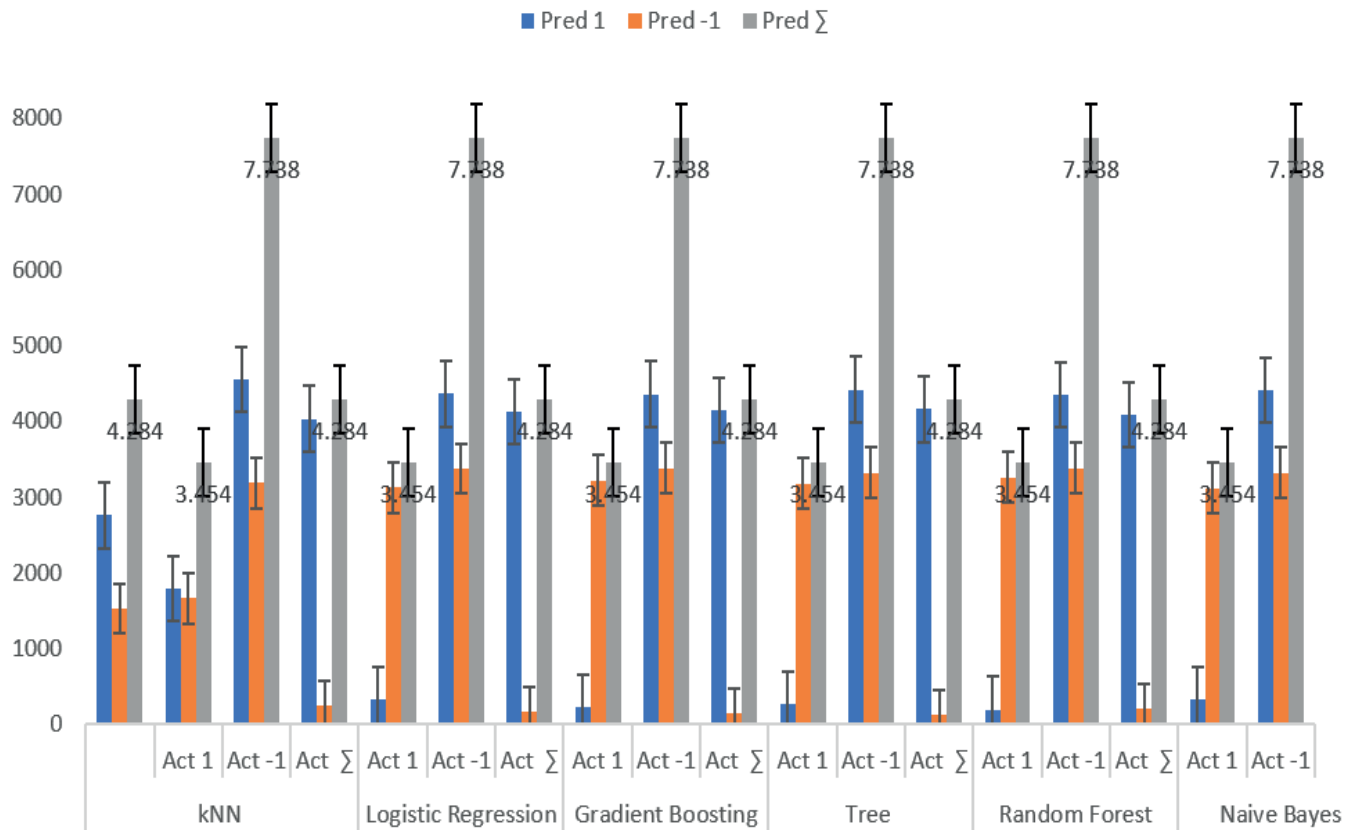


Figure 6. Confusion Matrix

Insights and Implications seem to substantiate the findings regarding constancy across models and predictability. The same aggregate performance indicates a balance between the use of the dataset and a balance in the weight matrix during evaluation. Another consistent finding is the difference of 830 between the Preds which always highlights the stronger nature of the Pred 1 biased across all models which suggests strong bias or class dependency whilst or after using the dataset. Even bigger problems can be industrialized when theories don't distinguish between the variability of mask vectors of class specific primary or negative correlations inherited from Pred Σ and the greatly limited or negative correlation vectors inherited from Pred 1 and Pred -1 for the models class which do not change. While the relative order of all predictions broadly follows class distribution pronounced class or inter shrinks even over limits.

Finally critical zone changes that ignore the margins set by variability and the performance break points within shape will allow such weaknesses to expand.⁽⁴⁰⁾

To begin with, it is important to assess the possible presence of class imbalance since oversampling or under sampling or employing metrics which are weighted could make for a more accurate evaluation of the model. In order to compare models, the use of additional evaluation metrics along with visualizations such as confusion matrices and class specific performance metrics like precision, recall or F1 score might come in handy. The difference shown by the error bars for Pred 1 and Pred -1 suggest that there is need to investigate the performance of this model with respect to different splits or subsets of the data and identify the reasons for the differences that were observed. Lastly, in real-world settings, simpler models such as Logistics Regression and Naive Bayes may be preferred more if they are easier to interpret or cheaper to use computationally as long as their performance is still adequate for the needs of the application in question.

This analysis demonstrates the need for proper understanding of both class as well as aggregate predictions so as to enable an even formulation of model evaluations and mitigate real world problems.

CONCLUSION

In summary Phishing attacks still remain among the most strategic forms of attacks mounted at an organization

and or an individual, and they take advantage of users' trust and fake sites with the malicious intent to claw sensitive information from these users. The substantiation gathered from this research further adds credence to the claims that machine learning approaches are highly effective in combating the threats such attacks pose. After examining a database consisting of original and phishing URLs, the study reveals how well machine learning algorithms can verify a website and thus serve as a defense against phishing. In this research, we used several machine learning models, notably, Random Forest, Gradient Boosting, and Support Vector Machines. However, the Random Forest model turned out to be the most powerful with the classification accuracy of 97,6 %. Likewise, Gradient Boosting also performed well, achieving high levels of precision and recall whilst being effective at detection capabilities. In this study feature selection is underscored to enhance performance of algorithms, Measures such as the length of a URL, age of the domain and the existence of HTTPS are indicated to be strong markers of phishing websites. These features contribute significantly to the performance of machine learning models in classifying sites as legitimate or malicious. An important advantage of this research is the practical direction on the development of the flexible and efficient system aimed at phishing detection.

The incorporation of machine learning increases accuracy while offering scalability which facilitates real time detection of phishing attacks. Such flexibility remains fundamental in the fight against cyber criminals who are always coming up with new ways of outsmarting traditional security. However, this study has limitations and acknowledges them; such include a dependence on particular datasets and the suggested need for implementing optimization in feature engineering. Explore more world-renowned datasets as well as other ideologies such as deep learning should be done in their advanced algorithm development to improve the detection aspects more so. Explainable AI methods should also be incorporated and ensemble models adopted to make automated systems more transparent and trustworthy so that users can understand the reason behind a certain classification. Hence, considering all aspects, the system once implemented will be evaluated with respect to performance metrics to measure how effective it is in counteracting phishing attacks. This paper suggests an all two-pronged approach to tackling phishing attacks considering both high end algorithms as well as data problems ensuring diversity in methods subsequently providing a in depth and robust solution. Survivors of the future fight against advancing phishing attacks may very well consider this research to be the holy grail. Not only does this research resolve contemporary problems regarding cyber security, but it also prepares the battleground for later advancements in the detection of phishing systems.

REFERENCES

1. Al-batah M, Al-Batah M, Salem Alzboon M, Alzaghoul E. Automated Quantification of Vesicoureteral Reflux using Machine Learning with Advancing Diagnostic Precision. *Data Metadata* [Internet]. 2025 Jan 1;4:460. Available from: <http://dx.doi.org/10.56294/dm2025460>
2. Abdel Wahed M, Alqaraleh M, Salem Alzboon M, Subhi Al-Batah M. Application of Artificial Intelligence for Diagnosing Tumors in the Female Reproductive System: A Systematic Review. *Multidiscip* [Internet]. 2025 Jan;3:54. Available from: <http://dx.doi.org/10.62486/agmu202554>
3. Al-batah M, Al-Batah M, Salem Alzboon M, Alzaghoul E. Automated Quantification of Vesicoureteral Reflux using Machine Learning with Advancing Diagnostic Precision. *Data Metadata* [Internet]. 2025 Jan 1;4:460. Available from: <https://dm.ageditor.ar/index.php/dm/article/view/460>
4. Alqaraleh M, Salem Alzboon M, Mohammad SA-B. Optimizing Resource Discovery in Grid Computing: A Hierarchical and Weighted Approach with Behavioral Modeling. *LatIA* [Internet]. 2025 Jan 1;3:97. Available from: <http://dx.doi.org/10.62486/latia202597>
5. Wahed MA, Alqaraleh M, Salem Alzboon M, Subhi Al-Batah M. Evaluating AI and Machine Learning Models in Breast Cancer Detection: A Review of Convolutional Neural Networks (CNN) and Global Research Trends. *LatIA* [Internet]. 2025 Jan 1;3:117. Available from: <http://dx.doi.org/10.62486/latia2025117>
6. Al-Batah M, Salem Alzboon M, Alqaraleh M. Superior Classification of Brain Cancer Types Through Machine Learning Techniques Applied to Magnetic Resonance Imaging. *Data Metadata* [Internet]. 2025 Jan 1;4:472. Available from: <http://dx.doi.org/10.56294/dm2025472>
7. Alzboon MS, Alzboon MS. From Complexity to Clarity: Improving Microarray Classification with Correlation-Based Feature Selection. *LatIA*. 2025;
8. Retraction: Phishing website detection using machine learning and deep learning techniques (J. Phys.: Conf. Ser. 1916 012169). *J Phys Conf Ser* [Internet]. 2021 May 1;1916(1):012407. Available from: <https://>

iopscience.iop.org/article/10.1088/1742-6596/1916/1/012407

9. Alqaraleh M, Salem Alzboon M, Subhi Al-Batah M, Solayman Migdadi H. From Complexity to Clarity: Improving Microarray Classification with Correlation-Based Feature Selection. *LatIA [Internet]*. 2025 Jan 1;3:84. Available from: <http://dx.doi.org/10.62486/latia202584>

10. Kasim S, Valliani N, Ki Wong NK, Samadi S, Watkins L, Rubin A. Cybersecurity as a Tic-Tac-Toe Game Using Autonomous Forwards (Attacking) And Backwards (Defending) Penetration Testing in a Cyber Adversarial Artificial Intelligence System. In: *ICOSNIKOM 2022 - 2022 IEEE International Conference of Computer Science and Information Technology: Boundary Free: Preparing Indonesia for Metaverse Society*. 2022.

11. Alqaraleh M, Salem Alzboon M, Subhi Al-Batah M. Real-Time UAV Recognition Through Advanced Machine Learning for Enhanced Military Surveillance. *Gamification Augment Real [Internet]*. 2025 Jan 1;3:63. Available from: <http://dx.doi.org/10.56294/gr202563>

12. Baliyan H, Prasath AR. Enhancing Phishing Website Detection Using Ensemble Machine Learning Models. *2024 OPJU Int Technol Conf Smart Comput Innov Adv Ind* 40. 2024;

13. Jain M, Rattan K, Sharma D, Goel K, Gupta N. Phishing Website Detection System Using Machine Learning. *J Netw Commun Syst*. 2024;

14. Pathmanaban J, James PG, Ashok P, Ragesh B, Aakash S, Kaushik N. Phishing Website Detection Using Machine Learning. *Proc 2nd IEEE Int Conf Netw Commun 2024, ICNWC 2024*. 2024;

15. U S SS. Phishing Website Detection using Machine Learning. *Interantional J Sci Res Eng Manag*. 2024;08(06):1-5.

16. Alazaidah R, Al-Shaikh A, AL-Mousa MR, Khafajah H, Samara G, Alzyoud M, et al. Website Phishing Detection Using Machine Learning Techniques. *J Stat Appl Probab [Internet]*. 2024 Jan 1;13(1):119-29. Available from: <https://digitalcommons.aaru.edu.jo/jsap/vol13/iss1/8/>

17. Wahed MA, Alqaraleh M, Alzboon MS, Al-Batah MS. Application of Artificial Intelligence for Diagnosing Tumors in the Female Reproductive System: A Systematic Review. *Multidiscip*. 2025;3:54.

18. Wahed MA, Alqaraleh M, Alzboon MS, Subhi Al-Batah M, de la Salud R el C, la de la Inteligencia T. AI Rx: Revolutionizing Healthcare Through Intelligence, Innovation, and Ethics. *Semin Med Writ Educ [Internet]*. 2025 Jan 1;4(35):35. Available from: <http://dx.doi.org/10.56294/mw202535>

19. Prayogo RD, Alfisyahrin AR, Gambetta W, Karimah SA, Nambo H. An Explainable Machine Learning-Based Phishing Website Detection using Gradient Boosting. In: *Proceeding - 2024 International Conference on Information Technology Research and Innovation, ICITRI 2024 [Internet]*. IEEE; 2024. p. 76-81. Available from: <https://ieeexplore.ieee.org/document/10698870/>

20. Mahalakshmi S, Meena P, Gopinath MR. Detection of Phishing Website Using Machine Learning. *Int J Res Publ Rev*. 2024;5(2):1817-21.

21. Carrasco Ramírez JG. AI in Healthcare: Revolutionizing Patient Care with Predictive Analytics and Decision Support Systems. *J Artif Intell Gen Sci* ISSN3006-4023. 2024;1(1):31-7.

22. Vaishnavi Bhojar, Komal Dharak, Dipali Gawali. Detection of Phishing Website using Machine Learning. *Int J Adv Res Sci Commun Technol [Internet]*. 2024 Jan 7;26-7. Available from: <http://ijarsct.co.in/Paper15004.pdf>

23. Al saedi M, Abbas Flayh N. Phishing Website Detection Using Machine Learning: A Review. *Wasit J Pure Sci*. 2023;2(2):270-81.

24. Kashyap S. The Influence of Artificial Intelligence on Cybersecurity. *Int J Innov Res Comput Commun Eng*. 2024;12(Special Is):13-22.

25. Subashini K, Narmatha V. Phishing Website Detection using Hyper-parameter Optimization and Comparison of Cross-validation in Machine Learning Based Solution. In: 2023 3rd International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies, ICAECT 2023. 2023.

26. Al-Batah M, Salem Alzboon M, Alqaraleh M, Ahmad Alzaghoul F. Comparative Analysis of Advanced Data Mining Methods for Enhancing Medical Diagnosis and Prognosis. *Data Metadata* [Internet]. 2024 Oct 29;3(3):83-92. Available from: <http://dx.doi.org/10.56294/dm2024.465>

27. Al-shanableh N, Alzyoud M, Al-husban RY, Alshanableh NM, Al-Oun A, Al-Batah MS, et al. Advanced Ensemble Machine Learning Techniques for Optimizing Diabetes Mellitus Prognostication: A Detailed Examination of Hospital Data. *Data Metadata* [Internet]. 2024 Sep 2;3. Available from: <http://dx.doi.org/10.56294/dm2024.363>

28. Muhyeeddin A, Mowafaq SA, Al-Batah MS, Mutaz AW. Advancing Medical Image Analysis: The Role of Adaptive Optimization Techniques in Enhancing COVID-19 Detection, Lung Infection, and Tumor Segmentation. *LatIA* [Internet]. 2024 Sep 29;2:74. Available from: <http://dx.doi.org/10.62486/latia202474>

29. Alqaraleh M, Alzboon MS, Al-Batah MS. Skywatch: Advanced Machine Learning Techniques for Distinguishing UAVs from Birds in Airspace Security. *Int J Adv Comput Sci Appl* [Internet]. 2024;15(11):1065-78. Available from: <http://dx.doi.org/10.14569/IJACSA.2024.01511104>

30. Alqaraleh M, Alzboon MS, Al-Batah MS, Abdel Wahed M, Abuashour A, Alsmadi FH. Harnessing Machine Learning for Quantifying Vesicoureteral Reflux: A Promising Approach for Objective Assessment. *Int J Online Biomed Eng* [Internet]. 2024 Aug 8;20(11):123-45. Available from: <https://online-journals.org/index.php/i-joe/article/view/49673>

31. Abuashour A, Salem Alzboon M, Kamel Alqaraleh M, Abuashour A. Comparative Study of Classification Mechanisms of Machine Learning on Multiple Data Mining Tool Kits. *Am J Biomed Sci Res* 2024 [Internet]. 2024;22(1):1. Available from: www.biomedgrid.com

32. Alzboon MS, Bader AF, Abuashour A, Alqaraleh MK, Zaqaibeh B, Al-Batah M. The Two Sides of AI in Cybersecurity: Opportunities and Challenges. In: 2023 International Conference on Intelligent Computing and Next Generation Networks (ICNGN) [Internet]. IEEE; 2023. p. 1-9. Available from: <https://ieeexplore.ieee.org/document/10396670/>

33. Alzboon MS, Qawasmeh S, Alqaraleh M, Abuashour A, Bader AF, Al-Batah M. Pushing the Envelope: Investigating the Potential and Limitations of ChatGPT and Artificial Intelligence in Advancing Computer Science Research. In: 2023 3rd International Conference on Emerging Smart Technologies and Applications (eSmarTA) [Internet]. IEEE; 2023. p. 1-6. Available from: <https://ieeexplore.ieee.org/document/10293294/>

34. Alzboon MS, Al-Batah MS. Prostate Cancer Detection and Analysis using Advanced Machine Learning. *Int J Adv Comput Sci Appl* [Internet]. 2023;14(8):388-96. Available from: <http://thesai.org/Publications/ViewPaper?Volume=14&Issue=8&Code=IJACSA&SerialNo=43>

35. Alzboon MS, Al-Batah MS, Alqaraleh M, Abuashour A, Bader AFH. Early Diagnosis of Diabetes: A Comparison of Machine Learning Methods. *Int J online Biomed Eng*. 2023;19(15):144-65.

36. Alzboon MS, Qawasmeh S, Alqaraleh M, Abuashour A, Bader AF, Al-Batah M. Machine Learning Classification Algorithms for Accurate Breast Cancer Diagnosis. In: 2023 3rd International Conference on Emerging Smart Technologies and Applications (eSmarTA) [Internet]. IEEE; 2023. p. 1-8. Available from: <https://ieeexplore.ieee.org/document/10293415/>

37. Putri AK, Alzboon MS. Doctor Adam Talib's Public Relations Strategy in Improving the Quality of Patient Service. *Sinergi Int J Commun Sci* [Internet]. 2023 May 25;1(1):42-54. Available from: <https://journal.sinergi.or.id/index.php/ijcs/article/view/19>

38. Al-Batah MS, Alzboon MS, Alazaidah R. Intelligent Heart Disease Prediction System with Applications in Jordanian Hospitals. *Int J Adv Comput Sci Appl* [Internet]. 2023;14(9):508-17. Available from: <http://thesai.org/Publications/ViewPaper?Volume=14&Issue=9&Code=IJACSA&SerialNo=54>

39. Alzboon MS, Al-Batah M, Alqaraleh M, Abuashour A, Bader AF. A Comparative Study of Machine Learning Techniques for Early Prediction of Diabetes. In: 2023 IEEE Tenth International Conference on Communications and Networking (ComNet) [Internet]. IEEE; 2023. p. 1-12. Available from: <https://ieeexplore.ieee.org/document/10366688/>

40. Alzboon MS. Survey on Patient Health Monitoring System Based on Internet of Things. *Inf Sci Lett* [Internet]. 2022 Jul 1;11(4):1183-90. Available from: <https://www.naturalspublishing.com/Article.asp?ArtcID=25233>

FINANCING

Currently, there are no available financing sources designated for this project. This absence of financial support underscores the need for strategic planning to identify potential funding avenues that could facilitate the successful implementation and advancement of the initiative.

CONFLICT OF INTEREST

The authors declare that the research was conducted without any commercial or financial relationships that could be construed as a potential conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Mowafaq Salem Alzboon, Mohammad Al-Batah.

Data curation: Muhyeeddin Alqaraleh.

Software: Mohammad Al-Batah, Muhyeeddin Alqaraleh, Faisal Alzboon, Lujin Alzboon.

Data analysis: Muhyeeddin Alqaraleh and Mowafaq Salem Alzboon.

Funding acquisition: Mowafaq Salem Alzboon, Mohammad Al-Batah.

Project supervision: Mowafaq Salem Alzboon, Mohammad Al-Batah.

Writhing - Original Draft: Mowafaq Salem Alzboon, Mohammad Subhi Al-Batah, Muhyeeddin Alqaraleh, Faisal Alzboon, Lujin Alzboon.

Writhing - Proofreading and editing: Mowafaq Salem Alzboon, Mohammad Subhi Al-Batah, Muhyeeddin Alqaraleh, Faisal Alzboon, Lujin Alzboon.