National College of Ireland

Project Submission Sheet

Student Name:	Matthew Browne		
Student ID:	x21174415@student.ncirl.ie		
Programme:	MSc/PGD in Cybersecurity	**Year:**	1
Module:	AI/ML in Cybersecurity (H9AIMLC)		
Lecturer:	Jaswinder Singh MSc/PGD		
Submission Due Date:	19th October 2025		
Project Title:	"How Can Machine Learning and Artificial Intelligence Be Used to Identify Malicious URLs, And How Does This Solve the Issue of a Safer Online Experience".		
Word Count:	5614		

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the references section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

Signature: Matthew Browne

Date: 19th October 2025

PLEASE READ THE FOLLOWING INSTRUCTIONS:

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. Projects should be submitted to your Programme Coordinator.
3. **You must ensure that you retain a HARD COPY of ALL projects**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.
4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. **Late submissions will incur penalties.**

5. All projects must be submitted and passed in order to successfully complete the year. **Any project/assignment not submitted will be marked as a fail.**

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

AI Acknowledgement Supplement

[AI/ML in Cybersecurity (H9AIMLC)

Your Name/Student Number	Course	Date
Name: Matthew Browne Student Number: x21174415	MSc/PGD in Cybersecurity	19/10/2025

This section is a supplement to the main assignment, to be used if AI was used in any capacity in the creation of your assignment; if you have queries about how to do this, please contact your lecturer. For an example of how to fill these sections out, please click here.

AI Acknowledgment

This section acknowledges the AI tools that were utilized in the process of completing this assignment.

Tool Name	Brief Description	Link to tool
Not Applicable		

Description of AI Usage

This section provides a more detailed description of how the AI tools were used in the assignment. It includes information about the prompts given to the AI tool, the responses received, and how these responses were utilized or modified in the assignment. **One table should be used for each tool used**.

Not Applicable	

Evidence of AI Usage

This section includes evidence of significant prompts and responses used or generated through the AI tool. It should provide a clear understanding of the extent to which the AI tool was used in the assignment. Evidence may be attached via screenshots or text.

Additional Evidence:

[Place evidence here]

Not Applicable	

Continuous Assessment Name	Part 1 Proposal, "How Can Machine Learning and Artificial Intelligence Be Used to Identify Malicious URLs, And How Does This Solve the Issue of a Safer Online Experience."
Student Name	Matthew Browne
Student ID	x21174415
Student Email	x21174415@student.ncirl.ie

"How Can Machine Learning and Artificial Intelligence Be Used to Identify Malicious URLs, And How Does This Solve the Issue of a Safer Online Experience"

Matthew Browne
MSc/PGD in Cybersecurity
E-mail *x21174415@student.ncirl.ie*

Contents

Abstract

Based on the requirements of our continues assessment for AI and Machine Learning we were required to think about an area where Artificial intelligence and machine learning could be applied in the real world to help mitigate or solve an issue that we as Cybersecurity Professionals see day to day, which would be a benefit to industry. With this in mind and having worked in IT for 15+ years detecting analyzing and responding to alerts is a continuous boring cycle and often can be described as mundane challenge and task. This is something we face every day being able to respond appropriately to these alerts in a timely and efficient manner is which key to keeping our infrastructure safe and secure. For my project I've chosen to research understand and analyse how phishing prevention and detection of deceptive URL's can help with the day-to-day safety online systems weather it's through social media sites, video sharing sites, or ecommerce payment sites. Standard run of the mill users doesn't realise these malicious URLs can cause significant harm to both their personal home systems and enterprise managed workstations and can have a negative financial impact should they fall victim to malicious URL's.

This is where inspecting these malicious URLs using machine learning and artificial intelligence can provide for both a business benefit and a safer internet experience at home and at work ensuring users don't get scammed. The research aims to look at how we do this by classifying dangerous sites, Using Indicators of compromise, warning users with banners in email, and training both users and our AI detection systems on link hygiene and integrating intrusion preventions systems within our Av and Firewall products with the use of advanced AI And ML tooling's at lightning speeds. We look at how AI can contribute to addressing these concerns in real life situations. Where I got the inspiration for this was from a future trends blog post on Fortinet's website which discussed how AI and ML could be used to identify phishing URLs faster for protection of users online. [1]

When we think about AI and ML we think as developers how we can train these datasets by using open-source technologies and allowing AI to guide us towards a safer, more secure browsing experience which we later understand as a combination of supervised and unsupervised learning techniques.

I. Introduction

One of the most frustrating about working in cybersecurity is how common both individuals and organizations come across malicious URL's and how these URL's become the starting point for many cyber incidents both at home and in the office , my research paper begins by asking the question to think about ways both Machine Learning and Artificial Intelligence can provide for a beneficial way to prevent these types of attacks from happening and how implementing these into a solution can provide a value add for the industry , with this in mind I began to think about what if AI And ML could be introduced as a more preventative method as part of a safer online feature and experience , this would essentially solve a costly issue which could be described as for most people and security professionals as valuable in the industry. As with many IT teams and the adoption of soc and siem tooling across industries we have seen an uplift in the amount of ransomware attacks happening or at least starting because of people clicking links in email's , video's , social media sites and these malicious links are becoming more and more sophisticated with this happening at a high rate in the world we need to begin to think about a way in which we can prevent this from happening.

Could training AI And ML to identify new and existing malicious links be the way of the future for providing this business and personal benefit to keeping people and organizations safer online? Possibly but only if we can do something with it , that's where my research piece plays an integral part of the whole hypothesis for my project I want to try and understand how the prevention of deceptive URL's can be combated using both AI And ML but not just to use them to actually leverage them in a way that can provide for a safer online experience , with that in mind I look to expand my purview and set out on an exploratory research piece where bring both AI and ML together to be able to classify these malicious URL's before a an individual clicks into them , this provides a business benefit for the individual and organization and also looks to solve a worrying trend in the industry which is Malicious Links are causing negative and financial impacts amongst organizations and individuals , ultimately leading to higher ransom payments which in turn funds organized crime.

Being able to inspect these malicious URLs using AI And ML while training the systems against new and existing indicators of compromise will allow individuals to and organizations to bring together new features within their existing systems, leverage them for a safer online experience and prevent them from being ultimately scammed online therefore ensuring crime and fraud are lowered for both the general consumer and the organization. The kicker here it to intertwine how the AI and ML algorithms does this , does it use IOC'S , Supervised or un Supervise learning techniques , are there other algorithms and techniques it can use all of this combines to form part of the research which ill conduct to assess essentially "How Can Machine Learning and Artificial Intelligence Be Used to Identify Malicious URL'S and How Does This Solve the Issue of a Safer Online Experience" As an Avid reader and technologist I've always enjoyed exploring these types of scenarios and hypotheses so this brings together an analysis of what the issue is in the real world , how it can address an industry wide issue which is dangers , malicious activity , financial burdens and more and where technologies can be used to benefit and support individuals it ultimately helps us understand how we can gain from using it train those data sets to be more beneficial in keeping us and giving us a safer online experience , this bring us over to our Motivation for the research paper.

II. Motivation

Phishing attacks have become more common than ever before nearly becoming the norm, with more a more people, companies, institutions and individuals being targeted, no one is safe from them. Every day more and more individuals are being exploited by malicious actors through sophisticated phishing attempts, these attempts by activists and hacktivists look to prey on vulnerable people who are not technology savvy, incite a sense of urgency and fear, this ultimately results in people clicking these fraudulent links and getting extorted deeply affecting livelihoods.

Although companies and individuals look to implement preventative measures like safe links detection, blacklist blocks the adversaries are becoming more and more difficult to track and stop. Traditional preventative measures are no longer standing up to these advanced attacks. Essentially the methods which previously worked to defend against these type of attacks are no longer adequate and therefore fighting these has become increasingly difficult. Both Machine Learning and Artificial intelligence advancements are finally making waves in these defenses, while not perfect and very much a work in progress there giving companies and individuals a way to differentiate against what's safe and what isn't. Machine learning algorithms and techniques give us a way to begin to understand what's publicly known as malicious and what could be considered a new threat or attack method, this allows us to categories the threats as they begin to emerge with the use of newer detection methods like indicators of compromise , if we can train these algorithms in a user friendly way were able to provide a business benefit for both personal and enterprise use of Artificial intelligence and Machine Learning e.g. of this might be to use co-pilot to verify and check links before we click on them to alert us to a true threat or a negative threat. If we can teach these agents to identify the threats faster, more efficiently and easier for the end user we can keep people safe online.

My research project aims to understand how both Machine Learning and Artificial Intelligence can be used to identify malicious URLs to keep individuals safe online. As part of the research, I'll be looking at how Machine Learning can be trained against these data sets to understand known and unknown URL's and how Artificial Intelligence can aid in the categorization of the URLs. My project essentially looks to analyse how Machine Learning is trained against the data sets being used and then how Artificial intelligence provides a value add to the categorizations of the URLs as there analyzed.

III. Research Question

My Research Question for the paper was selected based on how much of an inconvenience and frustration malicious URL's can be for both an organization and individual its titled:

"How Can Machine Learning and Artificial Intelligence Be Used to Identify Malicious URL'S and How Does This Solve the Issue of a Safer Online Experience"

IV. Initial Review

With the growing concerns and controversy around malicious and dangerous URLs found in everyday email threads, social media postings and online advertisements alongside additional academic research papers people are finding it more and more difficult to differentiate between what is real and what is fake due to the complexity and advance nature of new phishing techniques. Despite the high level funding which goes into educating people and the campaigns around cyber safety both organizations and individuals are continuing to face escalated security concerns and challenges in the face of adversity attack techniques are just becoming two sophisticated and people cannot keep up this is reflected in the extensive research I have been able to do in picking my seven research papers for analysis.

Based on the analysis of the seven research papers I can see that trying to identify the pattern into detecting the dangerous URLs using machine learning algorithms and delving into the model types behind these showcases that deep learning techniques is very much an in demand requirement across the research these techniques all combine to provide for an enhancement to the overall defence capabilities which in turn keeps us safer online. By bringing together the different outputs of the studies and surveys conducted I was able to gain different perspectives on how AI and ML could be used in identifying, classifying and mitigating against malicious URLs, this shows us that by using a combination of both we should be able to mitigate cyber threats while contributing to a safer online experience.

With that in mind we can see and its evident from the papers that malicious URLs are a continues never ending lifecycle of problems and risks the research tells me that improving detection capabilities, refining efficiency around analysis and ensuring reliability of the AI and ML all play a significant role in the process of identifying these dangerous URL's,

The "URL Net" [6] research paper showed me that they were looking at new way to detect against new malicious URLs with the power of machine learning , due to the fact that the traditional machine learning methods wouldn't work as they were just blacklists collected by multiple vendors in a crowd sourcing fashion as part of av products , this was proving ineffective against newer malicious URL's to combat this deep learning framework was introduced and or created to assess the "lexical properties" of URL strings this allowed for modern way of collecting multiple bits of information in the URL string enabling researchers to introduce additional model like SVM'S to take care of the recognition by learning directly from the strings themselves , this essentially fixed the issue whereby previously there was a need for manual assessment of the URLs moving to a more fluid and automated method of identifying the malicious URL's this sparked an inquisitive interest for me into understanding this further.

Another paper which peaked further interest was the survey paper for "Malicious URL's using Machine learning techniques" [3] For this survey paper we got a better understanding of what " lexical" meant as a feature , it discussed how a URL would normally look , what data is available in it such as where its hosted and what content would be held in the URL e.g. what might the url contain such as its page contents of the webpage itself , by explaining to us what different features are picked up in the webpage url it highlighted how the different features can effect the speed at which a malicious url can be identified and why as more and more features are scanned depending on the quantity it could become more difficult for model to rely on extracting these features for identification of the malicious URLs.

Additional to this I could see by looking at some other research papers like “Feature Extraction and Machine Learning” [2] , “Malicious URL Detection Using Machine Learning” [4] and “Enhancing Malicious URL Detection” [7]

These all had a keen focus on improving the accuracy of identification of malicious URL’s they specifically spoke to the types of machine learning models which could help in this such as “hybrid” and “ensemble” alongside the model types they also spoke about how the algorithms could be combined such as “Random Forests” and “LSTM’s this would allow them to capture the contents and structure of the URL’s and identify the patterns , the key thing here was by combining the algorithms together they were more efficient and robust then using them separately. Looking at some of the research papers e.g. “Leveraging diverse and efficient ensemble machine learning “[9] and “Detecting Phishing URLs Based on a Deep Learning Approach” [10] I was able to understand model robustness kept coming up and how using algorithms of machine learning by themselves was not strong enough especially when so many remained static, understanding that attackers don’t use the same techniques day in and day out goes to the understanding of how you can explain the process and how might an attacker look to fool the trained model or data and create crafty URLs which could mislead training models which were static. From these papers and some of the others we as analysts now understand in newer systems a more understandable model is used like “lime with tabular data” [11] this essentially is an ensemble learning method which in turn explains why a url would be flagged.

Across all the research paper it’s apparent they include key elements required for this to work like deep learning models , if we are to succeed in being able to rapidly assess malicious URL’s this can only be achieved by combining more than one algorithm at a time as single machine learning algorithms don’t stand a chance against URLs which are constantly changing , with these models and algorithms comes other caveats as well such as the speed of the transitions and accuracy around how well the AI and ML can trusted when used to highlight the unsuspecting URL’s , its only when this is achieved will both AI and ML be useful in actually providing a safer online experience for end users. With that being said my research question is around “How Can Machine Learning and Artificial Intelligence Be Used to Identify Malicious URL’S How Does This Solve the Issue of a Safer Online Experience” , so as long as we can answer the how it can be used for identification preliminarily its looking like through a combination of deep learning, models , multiple algorithms and more bit by bit understanding of what data lies within the urls themselves. It’s only when we asses this can we truly understand the benefit of online safety with AI And ML at the centre of the answer.

V. Data Sources and Statistics

For my Research paper I will be using different types of URL’s both malicious and benign. As my data set source, I’ll be using “Kaggle” [12], I’m hoping that each sample I’ve chosen when doing the research will work as expected but more on that later, the data set itself contains thousand of url samples so ill pick a few and see what data and structure I get from them. For this to work correctly I’m going to need also include two forms of unbiased data set references first one ill use will be the “Phish Tank Database” [13] this gives me confirmed acceptance of verified phishing URLs alongside this ill also use the “UC Machine Learning Repository” [14] , this will show me attributes in the urls being used like the url domain Ip address , age and ranking on google . Both of these will allow me to showcase a range of views into the types of phishing links and will help me to diversify and showcase the different behaviours ill observe by using different types of links just like an end user would when they visit safe and malicious websites. For some of the testing and examples I’ll be bringing two data sets together , how ill achieve this is by using “Pandas” [15] showing things like eliminating duplicates within the datasets, changing url links by taking out and updating characters and looking at how I could change some of the url attributes to work with ML models , the data will be then split up into training data , validated data and test data these will be the three subsets.

VI. Machine Learning Methods

My research project brief is to look at three different types of machine learning methods/models which could be used to aiding in the identification of malicious URLs , links like malware , scams , fraud etc. , by choosing different methods for this I’m able to assess and understand how Random Forest which is a traditional method , CNN which is a deep learning approach and Gradient Boosting which is essentially a boosted model , all give me different validation viewpoints into how both AI And ML work together to support my research question in keeping people safe online by being used in tandem to identify malicious links.

- Method 01, “Random Forest Algorithm” [16]

  From researching Random Forest, the way I understood it was that if you were to look at in the context of a web link and then you were asked as a soc analyst to determine weather it was a good normal link or bad malicious link you would have a few things think about it take http://bank0fir3land.com vs https://www.bankofireland.com both links are similar but are very different at multiple points , here as an analyst you would look at the first bit http:// vs https:// clearly there’s a sign here something is wrong not malicious but just doesn’t start of good , the next piece is the www.bank0f vs www.bankof here we see the “o” letter has been replace with a “0” this is a second indicator something is off and finally the third error ir”3”land.com vs Ireland.com two very ending the ir”3”land.com is different to Ireland.com showing “e” was replaced with a “3” all of these are attributes that make up the url string as an analyst if you were being asked to look at this url you may have 1-3 different individuals determining the validity of it “Random Forest” essentially gathers up the three different analysts opinions on the subject of the url , these form different decision trees one might say it safe , the other may say its malicious and the third person may say there unsure , essentially random forest puts all these decision into yes/no answers and put them to a vote , if there more than one answer which comes out as yes the url is malicious then it takes that as the vote essentially combining decision trees and giving a calculated answer.

The reason I've chosen this as one of my algorithms is because it makes sense as it works with Tabular Data e.g. this link contains https and numbers, so it makes it an appropriate choice for testing. The second piece is that because it's essentially voting on the most collected answer it makes it easy to explain. It also serves as a good baseline model because if you can get a decision tree from something as simple as a incorrect link you can adapt it to more complex scenarios.

- Method 02, "Convolutional Neural Network" (CNN) [17]

  From researching CNN I've been able to gather that the background for this was based on how "humans began to learn patterns all by themselves" [19] in my research case this could be applied to urls as well, let's take the example I spoke about earlier vs https://www. bankofireland.com vs http://bank0fir3land.com both of these are perfect examples for these explanations as humans we know that our banking requirements must always be secure were taught this by the adverts they play on television , if we think about he we start to notice patterns e.g. http:// and https:// are two very different things one is secure one it not this is an example of how we train our eyes to notice these things even though both look very similar they don't have the same output CNN will look for things that shouldn't be in the url like bank"0"fir"3"land here we see two different incorrect characters in the url address itself these are more indicators that the url is malicious CNN looks for character text that shouldn't be in the url just like the way we scan a computer monitor banking login screen with our eyes , it does the same thing.

  The reason I've chosen this as one of my algorithms is because its relatable and easier to understand if you put it in the context of the ML being your eyes it does exactly the same thing and looks of patterns and mistakes making it a useful preventative measure in identifying malicious urls. The second reason just like our eyes tell our brain when somethings wrong it essentially trains itself making it an ideal detective measure as it learns by itself. And the third reason is because if we think about it our eyes tell our brain when something is wrong, CNN does the exact same thing the difference being it uses the self-awareness and discovery within scanning text to solve the problem just like our eyes do.

- Method 03, "Gradient Boosting" [18]

  From researching Gradient Boosting this seems more like a Random Forest 2.0 , where this one differs is instead of collecting all the results and choosing the most voted for result it starts with the question , if you were to answer the question the first time and you said the http://bank0fir3land.com is not malicious as the first security analyst , it then moves onto the next security analysts who may say it wasn't malicious so far we have one person saying it is and another saying it isn't , then it would move onto the final security analyst who may say there still unsure if it is or it isn't malicious "Gradient Bosting" builds out these scenarios one by one and then , after it build them out it tries to test against the scenarios to improve the final decision for each scenario , essentially if you had this as a phishing question in a quiz and you different analysts answered the same question three different ways it would highlight the correct analysts answers and the incorrect analysts answer but if the question came up again it would learn from previous mistakes meaning if the analysts got asked the same question again chances are the result would correct because its learned from its previous mistakes. , I'm using this to see how it stacks up against good and bad urls especially where answers will differ across the board and thirdly because like the other two it can be trained and speed and word work for my scenario.

VII. Evaluations Methods

Methods to be used in "Random Forest"

The way in which I'll evaluate Random Forest metrics is by using performance areas such as "Accuracy" "Precision" and " Recall" [20] These will allow me to achieve some measurable outcomes. "Accuracy" will allow me to understand the correct number of bad or good URLs which were classified, "Precision" will give me count of bad URLs which were definitely determined as bad, "Recall" will help me understand the measurement around how well the model actually detected these URLs. To visualize and understand the data ill be using a "Confusion Matrix" [21] This will help me understand what the model got correct for malicious URLs and what URLs were incorrect.

Methods to be used in "Convolutional Neural Network" (CNN)

I'll be using the same principles for the Convolutional Neural Network (CNN) analysis, the data set for this will remain the same based on our lecture videos we were shown that the dataset should be split into training, validation and test data "Accuracy", "Recall" and "Precision" performance metrics will be used just like I do for Random Forest. One additional piece of math's ill need for this is the "Area Under the Curve" [22] this will allow me to see how well CNN worked to separate the good URLs from the bad URLs. After I do this ill need to do similarly what I will have done with Random Forest to visualize the end result I'll do a "Confusion Matrix"*[21]* to understand the predictions the model made for the URLs good to bad ratio visualizations.

Method to be used in "XGBoost Evaluation"

Similar to my other two models ill be using "XGBoost" model , this two will be analyzed using "Precision" , "Recall" the slight twist here is ill be using what i learned about "AUC , Area Under The Curve " [22] for the other two with this one as well but ill be looking to test against the speed at which it can do the checks against the urls , this is because i want to understand how the performance matches up or if not should be better as "XGBoost" should learn from previous searches against a dataset , this will allow me to see how well it finds the malicious urls vs will the results be just as good and have the same accuracy as the other models.

VIII References

[1]Fortinet, "How Artificial Intelligence (AI) Can Help in Discovering Unknown Cybersecurity Threats," Fortinet, 2025. https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity. (accessed Oct. 07, 2025).

[2]Archive.org,2025. https://web.archive.org/web/20221221184752/https://drpress.org/ojs/index.php/HSET/article/download/3209/3091. (accessed Oct. 07, 2025).

[3] IEEE Xplore Full-TextPDF :, ieeexplore.ieee.org. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9950508. (accessed Oct. 07, 2025).

[4] Raed Bani Hani, Motasem Amoura, M. Ammourah, Yazeed Abu Khalil, and M. Swailm, "Malicious URL Detection Using Machine Learning," pp. 1–5, Aug. 2024, doi: https://doi.org/10.1109/icics63486.2024.10638299. (accessed Oct. 07, 2025).

[5] C.-I. Coste, "Using Ensemble Models for Malicious Web Links Detection," Proceedings of the 16th International Conference on Agents and Artificial Intelligence, pp. 657–664, 2024, doi: https://doi.org/10.5220/0012381800003636. (accessed Oct. 07, 2025).

[6] H. Le, Q. Pham, D. Sahoo, and S. Hoi, "URLNet: Learning a URL Representation with Deep Learning for Malicious URL Detection," 2018. Available: https://arxiv.org/pdf/1802.03162. (accessed Oct. 07, 2025).

[7] Hemanth Reddy Alavala, S. Singh, P. Joshi, and Sagar Basavaraju, "Enhancing Malicious URL Detection with Advanced Machine Learning Techniques," pp. 151–156, Feb. 2025, doi: https://doi.org/10.1109/ce2ct64011.2025.10939290. (accessed Oct. 07, 2025).

[8] L Shaheetha, K. Vadivazhagan, and M. Parvees, "Detection of Malicious Domains in the Cyberspace using Machine Learning & Deep Learning: A Survey," Dec. 2022, doi: https://doi.org/10.1109/smart55829.2022.10047254. (accessed Oct. 08, 2025).

[9] A. E. Omolara and M. Alawida, "DaE2: Unmasking malicious URLs by leveraging diverse and efficient ensemble machine learning for online security," Computers & Security, vol. 148, p. 104170, Jan. 2025, doi: https://doi.org/10.1016/j.cose.2024.104170. (accessed Oct. 08, 2025).

[10] E. ul H. Qazi, M. H. Faheem, and I. Ahmad, "Detecting Phishing URLs Based on a Deep Learning Approach to Prevent Cyber-Attacks," Applied Sciences, vol. 14, no. 22, pp. 10086–10086, Nov. 2024, doi: https://doi.org/10.3390/app142210086 . (accessed Oct. 08, 2025).

[11] GeeksforGeeks, "Explainable AI(XAI) Using LIME," GeeksforGeeks, Jan. 20, 2021. https://www.geeksforgeeks.org/artificial-intelligence/introduction-to-explainable-aixai-using-lime/ (accessed Oct. 08, 2025).

[12] "Malicious And Benign URLs," www.kaggle.com. https://www.kaggle.com/datasets/siddharthkumar25/malicious-and-benign-urls (accessed Oct. 08, 2025).

[13] "PhishTank | Join the fight against phishing," phishtank.org. https://phishtank.org/ (accessed Oct. 08, 2025).

[14] "UCI Machine Learning Repository," Uci.edu, 2025. https://archive.ics.uci.edu/dataset/187/url+reputation (accessed Oct. 08, 2025).

[15] Pandas, "Python Data Analysis Library," Pydata.org, 2018. https://pandas.pydata.org/ (accessed Oct. 08, 2025)

[16] GeeksforGeeks, "Random Forest Algorithm in Machine Learning," GeeksforGeeks, Feb. 22, 2024. https://www.geeksforgeeks.org/machine-learning/random-forest-algorithm-in-machine-learning/ (accessed Oct. 08, 2025)

[17] GeeksforGeeks, "Convolutional Neural Network (CNN) in Machine Learning," GeeksforGeeks, Dec. 25, 2020. https://www.geeksforgeeks.org/deep-learning/convolutional-neural-network-cnn-in-machine-learning/ (accessed Oct. 08, 2025)

[18] GeeksforGeeks, "Gradient Boosting in ML," GeeksforGeeks, Aug. 25, 2020. https://www.geeksforgeeks.org/machine-learning/ml-gradient-boosting/ (accessed Oct. 08, 2025)

[19] "Convolutional Neural Networks (CNNs) Explained | Beginner's Guide 2024," DxTalks, Digital Leaders Platform, May 16, 2024. https://www.dxtalks.com/blog/news-2/understanding-convolutional-neural-networks-cnns-a-beginner-s-guide-570 (accessed Oct. 09, 2025).

[20] "Welcome To Zscaler Directory Authentication," Byteplus.com, 2025. https://www.byteplus.com/en/topic/471927?title=how-to-measure-success-with-random-forests-a-comprehensive-guide (accessed Oct. 09, 2025).

[21] Wikipedia Contributors, "Confusion matrix," Wikipedia, Oct. 22, 2019. https://en.wikipedia.org/wiki/Confusion_matrix

[22] S. Kumar, "Area Under the Curve," *DEV Community*, Feb. 26, 2025. https://dev.to/shlok2740/area-under-the-curve-359c (accessed Oct. 09, 2025).