**A Model to Detect Phishing Attacks based Cybersecurity Threats and Vulnerabilities using Machine Learning Algorithm**

**By: Ebhabha Asuwa Kingsley**

# Hypothesis/Research Questions

The following are the specific study issues that we are attempting to answer:

RQ1: What are the security risks associated with machine learning-based software systems?

Deliverable: It will take 10 days.

RQ2: What are the most recent secure development techniques for machine learning-based software systems?

Deliverable: This task will take 15 days.

RQ3: How can machine learning detect phishing attacks from sites?

Deliverable: This task will take 15 days.

RQ4: What are the challenges and future directions for current practices in machine learning-based software systems? What are the present problems & prospects for machine learning-based software systems?

Deliverable: This task will take 15 days.

# The Problem / Short description of your idea

Cyber-attacks have become a more frequent hazard to humans and regular companies. Threat actors' methods and techniques have also evolved throughout the period. Cybersecurity is a developing concern that affects many aspects of society. Each attacker seems to have the ability to damage the systems on a massive scale. Typically, attackers will employ phishing to manipulate individuals in obtaining access to the company's digital content and networking. Cyber attackers use security flaws to launch ransomware attacks, gain illegal access, shut down systems, and even demand a fee to regain access. To mitigate against these vulnerabilities, several Artificial Intelligence (AI) techniques are deployed. Although threat awareness and cognitive analytics systems assist companies in detecting anomalous traffic patterns, the best approach for preventing phishing attempts is to respond in detail.

In this project, a model will be designed to detection of phishing attacks-based cyber threats using machine learning (ML) methods. For Machine learning processing, a standard legitimate dataset of phishing attacks from the Kaggle will be used. This methodology will help discover cybersecurity threats and vulnerabilities.

# The project aim(s)

This study aims to determine the best machine learning algorithm for detecting phishing attacks with the help of a standard legitimate dataset.

# The project objectives

The specific objectives of the study are as follows:

**Objective 1:** To address the issue of data over-fitting.

Deliverable: Chapter 3 in the project report, which will take 2 days.

**Objective 2:** To minimize the redundancy of data in the data collection that is irrelevant or unnecessary.

Deliverable: Chapter 3 in the project report, which will take 4 days.

**Objective 1:** To assess and choose standard legitimate datasets for classification and detection using standard classification and detection algorithms.

Deliverable: Chapter 5 in the project report, which will take 2 days.

**Objective 1:** To detect Phishing attacks using machine learning techniques.

Deliverable: Chapter 4 in the project report, which will take 8 days.

**Objective 1:** To assess performance and improve the accuracy of phishing attack detection by using machine learning techniques.

Deliverable: Chapter 5 in the report project, will take 10 days.

# Development tools

The suggested technique will make use of the python programming language, which will be implemented on the jupyter notebook platform, to serve as a simulation environment.

**Software Tool: Python**

Python is a great scripting language that places a strong emphasis on intelligibility. It is often regarded as being simple to learn while yet being capable of harnessing the power of systems-level computer languages when required. (Raschka et al., 2020). GitHub reports that the Python community has expanded greatly over the previous decade, with the major driving factor being "a rapidly-expanding population of data science experts as well as enthusiasts." As per the study, the Python community has grown dramatically over the last decade. Python's characteristics make it an excellent choice for data analytics: it is simple to learn, robust, legible, scalable, has a large number of libraries, can be integrated with other languages, and has a vibrant community and support system. Python data analysis libraries are available like TensorFlow, Keras, Scikit-learn, Theano, NumPy, Pandas, Matplotlib, etc. (Butwall et al., 2019).

**Simulation Platform: Jupyter Notebook**

One of the many open-source browser-based tools that may be used to create a virtual lab notebook for researchers is the Jupyter notebook. Interoperability and academic exchange are made easier since they can be read by machines and humans alike. Online repositories may house these notebooks and link them to other study artifacts including datasets, code, methodology documentation, processes, other publications. Jupyter notebooks may help make science more approachable. Besides text & code, rich material like images, video, and even HTML/JavaScript interactive widgets are all integrated into notebooks. (Pimentel et al., 2019).

# How to plan to conduct the research

To get private information from users like their address, aadhar number, PAN card number, credit/debit card number, and bank account information as well as their passwords for online shopping sites and other sites, phishing is a very dangerous way to get it. Because of a lack of internet security, many people have had their personal information stolen or phished over the internet. It is common for phishing attempts to utilize bogus emails or websites to trick people into divulging personal or financial information. Phishing attacks and the most current methods for defending against them are covered. By considering this perspective, a few studies that use the methods indicated will be evaluated and their findings will be summarised. Based on this literature review, the problem will be specified and formulated. then to overcome the identified problem will be resolved by implementing the proposed method. The results will be evaluated and compared to assess the proposed method's performance. Then a deep discussion will be provided in the next phase of this research. Finally, this work will be concluded by considering all aspects of this research. The last task is final report writing.

**Research Methodology:**

Machine learning is an effective method for reducing phishing assaults. ML techniques are useful for detecting phishing websites because it reduces to a straightforward classification issue. When training a machine learning algorithm for a learning-based detection technique, the data at hand must include phishing and legitimate website classes. To identify a phishing attempt, many classifiers are utilized. Before we will be applied to input data, data preprocessing, feature selection technique, and after this will be used to machine learning-based classification techniques. These steps are given below:

* **Data gathering:** Data gathering is critical for data analysis—for our study, we used datasets from kaggle.com. This research required the phishing dataset[[1]](#footnote-1). A standard legitimate dataset of phishing attacks from Kaggle will be used to help with ML processing. These records include both legitimate and phishing website instances.
* **Data acquisition:** The data is made up of characteristics taken from sets of website URLs. The supplied information will be gathered and processed to develop and access several classification algorithms for the task of identifying phishing websites based on URL attributes, URL resolving metrics, and external services. Because the supplied datasets include properties that can be readily retrieved, this dataset will assist academics and practitioners in quickly building classification models in solutions to avoid phishing attacks.
* **Pre-Processing:** Data pre-processing is a critical step in the ML application. It creates with raw data as well as structured using the data mining approach. In this step, data will be clean and noise-free by checking incomplete and missing values.
* **Feature selection:** The task of selecting features is critical for the analysis of the dataset. Our dataset has 32 characteristics. Depending on the information provided by the feature, it is possible to predict if they would be suspicious or malicious. In this respect, a different feature selection technique will be used that will maintain only relevant and essential features.
* **Machine Learning Classification Based Modeling:** A machine learning algorithm will be used to determine categorization and detect cyber-attacks. The dataset must already be trained to predict new information in this technique. The machine learning techniques will be utilized in this study to identify phishing attacks.

**Evaluation performance metrics:**

As I have mentioned that this project will be implemented using python programming. Now the question is how this implemented solution will be evaluated with existing solutions or methods. So, the answer to this question is that the implemented solution will be evaluated through some performance metrics, for example, Accuracy, precision, recall, and the F1 score will be utilized to evaluate performances that will be determined using the confusion matrix. A confusion matrix is a distinctive tabular arrangement used for performance projections.

# Project plan



|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Task\_Name | 08-02-22 | 01-03-22 | 09-03-22 | 24-03-22 | 02-04-22 | 16-04-22 | 29-04-22 | 03-05-22 |
| Research Proposal | **15 Days** |  |  |  |  |  |  |  |
| Introduction |  | **09 Days** |  |  |  |  |  |  |
| Literature Review |  |  | **15 Days** |  |  |  |  |  |
| Research Methodology |  |  |  | **8Days** |  |  |  |  |
| Experimented Results |  |  |  |  | **14Days** |  |  |  |
| Analysis and Result Discussion |  |  |  |  |  | **13 Days** |  |  |
| Conclusion and Future Direction |  |  |  |  |  |  | **5 Days** |  |
| Final Dissertation |  |  |  |  |  |  |  | **4 Days** |

**Gantt chart**

# References:

Abedin, N. F., Bawm, R., Sarwar, T., Saifuddin, M., Rahman, M. A., & Hossain, S. (2020). Phishing attack detection using machine learning classification techniques. *Proceedings of the 3rd International Conference on Intelligent Sustainable Systems, ICISS 2020*. https://doi.org/10.1109/ICISS49785.2020.9315895

Alam, M. N., Sarma, D., Lima, F. F., Saha, I., Ulfath, R. E., & Hossain, S. (2020). Phishing attacks detection using machine learning approach. *Proceedings of the 3rd International Conference on Smart Systems and Inventive Technology, ICSSIT 2020*. https://doi.org/10.1109/ICSSIT48917.2020.9214225

Basit, A., Zafar, M., Javed, A. R., & Jalil, Z. (2020). A Novel Ensemble Machine Learning Method to Detect Phishing Attack. *Proceedings - 2020 23rd IEEE International Multi-Topic Conference, INMIC 2020*. https://doi.org/10.1109/INMIC50486.2020.9318210

Butwall, M., Ranka, P., & Shah, S. (2019). Python in Field of Data Science: A Review. *International Journal of Computer Applications*. https://doi.org/10.5120/ijca2019919404

Nadar, V. K., Patel, B., Devmane, V., & Bhave, U. (2021). Detection of Phishing Websites Using Machine Learning Approach. *2021 2nd Global Conference for Advancement in Technology, GCAT 2021*. https://doi.org/10.1109/GCAT52182.2021.9587682

Pimentel, J. F., Murta, L., Braganholo, V., & Freire, J. (2019). A large-scale study about quality and reproducibility of jupyter notebooks. *IEEE International Working Conference on Mining Software Repositories*. https://doi.org/10.1109/MSR.2019.00077

Raschka, S., Patterson, J., & Nolet, C. (2020). Machine learning in python: Main developments and technology trends in data science, machine learning, and artificial intelligence. In *Information (Switzerland)*. https://doi.org/10.3390/info11040193

Ripa, S. P., Islam, F., & Arifuzzaman, M. (2021). The emergence threat of phishing attack and the detection techniques using machine learning models. *2021 International Conference on Automation, Control, and Mechatronics for Industry 4.0, ACMI 2021*. https://doi.org/10.1109/ACMI53878.2021.9528204

Sindhu, S., Patil, S. P., Sreevalsan, A., Rahman, F., & Saritha, A. N. (2020). Phishing detection using random forest, SVM, and neural network with backpropagation. *Proceedings of the International Conference on Smart Technologies in Computing, Electrical and Electronics, ICSTCEE 2020*. https://doi.org/10.1109/ICSTCEE49637.2020.9277256

1. https://www.kaggle.com/akashkr/phishing-website-dataset [↑](#footnote-ref-1)