Project Plan

Initial Project Vision

Comprehensive review of existing methods

An in-depth comparison of current phishing detection methods, including blacklist-based, heuristics, visual similarity-based and traditional machine learning-based methods.

Evaluate the pros and cons of these methods in terms of accuracy, adaptability, and effectiveness against zero-day phishing attacks.

Evaluation of existing tools

Analyze popular phishing detection tools and software used in browsers such as Google Chrome, Mozilla Firefox, and Apple Safari, as well as standalone security solutions.

Evaluate their performance, update mechanisms, and limitations in real-world scenarios.

Develop deep learning-based solutions

Design and implement an online phishing detection system using convolutional neural networks (CNN) and CNN/LSTM models.

Focus on leveraging URL characteristics and website content capabilities to increase detection rates and reduce false positives and negatives.

Comparative analysis

The newly developed deep learning based detection system is compared with existing methods and tools.

Highlights improvements in detection accuracy, adaptability to new phishing threats, and overall system robustness.

Demonstration of effectiveness

Provide empirical evidence through experiments and analysis of results to demonstrate the effectiveness of the proposed solution.

A variety of datasets are used to validate the model's performance, demonstrating its ability to detect newly generated phishing URLs and various phishing techniques.

Adapt to New Threats

Increase the adaptability of phishing detection systems to emerging phishing threats, thereby reducing the incidence of successful phishing attacks.

Project Objectives

Assess the limitations of traditional methods
Critically analyze the limitations of existing phishing detection methods, such as blacklist-based, heuristics, visual similarity-based and traditional machine learning-based methods

Explore deep learning for phishing detection
Investigate the potential of deep learning algorithms, specifically convolutional neural networks (CNN) and CNN/LSTM models, for phishing website detection.

Feature extraction and analysis
Develop a comprehensive set of phishing detection capabilities, including URL-based and content-based capabilities. Key features include URL length, top-level domain extraction, hostname presence, special characters, HTTPS usage, number and letter counting, URL shortening modes, IP address usage, and various HTML content elements.

Model development
Design and implement CNN and CNN/LSTM models to effectively detect phishing websites using extracted features.

Experimental evaluation
An experimental framework is established to evaluate the performance of the proposed model using different datasets.

Performance
Define and use appropriate metrics to evaluate model performance, such as accuracy, precision, recall, and F1 score.

Result analysis
Analyze the experimental results to understand the effectiveness of the proposed model in different scenarios.
The performance of the proposed deep learning based model is compared with existing phishing detection methods and tools.

Conclusion and future work
Summarizes the main findings and highlights the advantages of using deep learning for phishing detection.
Identify areas for future research, such as improving feature engineering, enhancing model interpretability, and exploring new deep learning architectures.

Project plan

Project Plan			
Task	**Expected Start Date**	**Expected Completion Date**	**Review/Product/Deliverables/Outcomes**
1. Initiation		8th Jan	• Project Initialisation
2. Review	9th Jan	29th Jan	• Review the project plan and scheduling • Searching the paper related to the project
3. Stage 1	30th Jan	18th Feb	• Find the dataset and Deep learning model • Research and compare different deep learning model • Demo and confirm the ai model
4. Stage 2	19th Feb	9th Mar	• Preload the website content • Phishing website detect feature • Export the dataset
5. Stage 3	10th Mar	31st Mar	• Finalized the Dataset • Finalized the model • Export the result for each of the Model
6. Assembly of complete final report	1st Apr	30th Apr	• Report

Communication plan

Regular meetings with the project supervisor will be planned to ensure the project is meeting goals

Initial Risk List

Privacy

Privacy Concerns: The extension needs to handle website preloading and scanning, which involves accessing and analyzing website content. Ensuring user privacy is protected and sensitive information is not mishandled or stored insecurely is essential.

Scanning algorithms

Risk

Limited Coverage: Scanning algorithms may not cover all possible security vulnerabilities or may miss specific types of vulnerabilities. This could result in certain types of security risks going undetected, leaving websites or applications exposed to potential threats.

Performance Impact: Sophisticated scanning algorithms may require significant computational resources, potentially impacting the performance of the system being scanned. Excessive resource usage can lead to slower response times, increased server load, or even system instability. Training data and testing data is not rich enough to demonstrate the concept used for the detection.

Address risks

There are many products on the website scanner. Different products using existing AI models will be compared. Such as WOT: Website Security Checker, Vulnerability Network Scanner, Duckduckgo Privacy Essentials, Malwarebytes Browser Guard, Trend Micro Check, etc. Their artificial intelligence model will be used as the basis for training material. Reduce time to build new models. The training data will be compiled from public vulnerability databases such as the National Vulnerability Database (NVD), Common Vulnerabilities and Exposures (CVE) or the Open Web Application Security Project (OWASP) Top 10, which can provide useful information on known vulnerabilities. valuable information and their characteristics.

Stage Plans

Stage 1			
Task	**Start Date**	**End**	**Product/Deliverables/Outcome**
Find the dataset	30th Jan	18th Feb	Find datasets from Zemodo, Mendeleym Data and Kaggle
Compare the dataset	10th Feb	18th Feb	Compare which dataset is available for url, content and combined version
Research Deep learning model	5th Feb	17st Feb	Research and study RNN, ANN, LSTM, CNN, GNN model. Then determine which model will be used in the project
Demo and test models	12nd Feb	17th Feb	Demo and test models
Confirm model	18th Feb	18th Feb	Confirmed that CNN and LSTM models will be used

Stage 2			
Task	**Start Date**	**End**	**Product/Deliverables/Outcome**
Preload the website content	19th Feb	23rd Feb	Write python to preload website content based on website url link
Phishing website detect feature - url	23rd Feb	29th Feb	Identify phishing website URL characteristics in python
Phishing website detect feature - content	1st Mar	7th Mar	Identify phishing website content characteristics in python
Combine the url feature and content dataset	8th Mar	9th Mar	Combine url features and content data sets

Stage 3			
Task	**Start Date**	**End**	**Product/Deliverables/Outcome**
Finalized the Dataset	10th Mar	31st Mar	Python script to complete identity phishing website functionality
Finalized the model	12th Mar	31st Mar	Python script for running CNN models and CNN-LSTM models
Start the script	14th Mar	31st Mar	Run and export the results of each model. Adjust the data set and plot area in the figure