PROJECT AND TEAM INFORMATION

Project Title

Machine Learning-Based Phishing Attack Detection.

Student / Team Information

Team Name: *Team #*	Tech shield CYBER-IV-T003
Team member 1 (Team Lead)	*Tomar, Ishita – 230221280* *ishitatomar1992@gmail.com* 
Team member 2	*Gupta, Anshu –23022478* *anshugupta699@gmail.com* 

Team member 3	*Singh, Dashpreet -230213889* *dashpreetsingh632@gmail.com* 
Team member 4	*Singh, Ishita -230221084* *ishitasingh0804@gmail.com* 

PROPOSAL DESCRIPTION

Motivation

Phishing attacks are one of the most common cybersecurity threats, tricking users into revealing sensitive information such as login credentials and financial details. Traditional rule- based phishing detection methods struggle to adapt to evolving attack patterns. These attacks exploit trust, posing as legitimate entities to steal passwords, credit card data, and confidential information, leading to financial loss, data breaches, and identity theft. The increasing sophistication of these attacks, including the use of social engineering and advanced technical deception, necessitates more dynamic and intelligent detection mechanisms. Consequently, the development of machine learning-based solutions offer a promising avenue for enhanced protection against these evolving threats. Addressing this challenge is crucial for safeguarding individuals and organisations in the digital landscape.

State of the Art / Current solution

Phishing attacks are currently tackled using a combination of technological defences and user education. Traditional approaches include identifying known phishing patterns within email content, headers, and URLs, as well as maintaining blacklists and whitelists of malicious or trusted sources. Email providers also contribute by filtering messages using rule-based systems and reputation analysis to detect spam and phishing indicators. More advanced techniques involve heuristic analysis to detect suspicious elements in emails and websites, behavioural analysis to monitor for unusual user activity, and reputation-based systems to evaluate the credibility of online entities. Alongside these measures, educating users to recognise and report phishing attempts remains essential. However, these conventional methods often struggle to keep pace with the constantly evolving and increasingly sophisticated tactics used by cyber criminals. This underscores the growing need for more adaptive and intelligent solutions, such as machine learning-based phishing detection systems.

Project Goals and Milestones

1. **Develop an ML-based system for phishing detection**: To create a machine learning system capable of identifying phishing websites and emails.
2. **Improve detection accuracy:** To achieve a higher level of accuracy in identifying phishing attacks compared to traditional rule-based methods.
3. **Reduce false positives**: To minimise the number of legitimate websites and emails incorrectly flagged as phishing.
4. **Enable real-time phishing detection**: To implement a system that can identify phishing attempts as they occur, preventing associated cyber fraud.
5. **Enhance cybersecurity**: To contribute to a stronger overall cyber security posture by providing more effective protection against phishing threats.

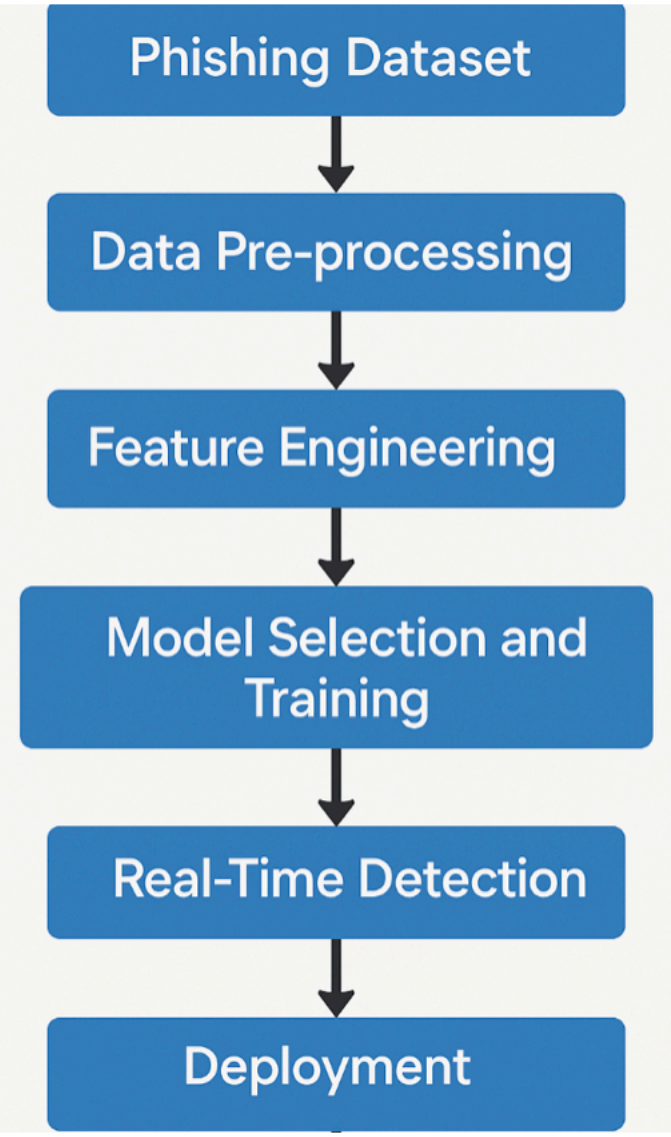
Project Approach

We will use Python as the programming language and develop an ML - based system to identify phishing websites and emails, improving detection accuracy and reduce false positives compared to traditional methods hence enabling real - time phishing detection to prevent cyber fraud associated with phishing attempts.

Project Workflow:

1. **Dataset Collection:** Begin by acquiring and preprocessing a comprehensive phishing dataset to ensure high data quality and relevance.
2. **Data Preprocessing**: Clean the dataset and normalise feature values to ensure consistency and improve model performance.
3. **Feature Extraction and Selection**:Apply feature selection techniques such as Information Gain, Chi-Square, and Recursive Feature Elimination (RFE) to identify and retain the most significant features for phishing detection.
4. **Model Selection**: Implement and compare multiple machine learning classifiers, including: Random Forest, XGBoost, Support Vector Machine (SVM), Logistic Regression, Naive Bayes
5. **Model Training and Evaluation**: Split the dataset into training and testing sets. Evaluate model performance using key metrics: Accuracy, Precision, Recall, F1-Score.
6. **Result Comparison**: Compare the performance of all algorithms to determine the most effective model for phishing detection. Visualise the results using tools such as confusion matrices, bar charts, and other relevant plots.

System Architecture (High Level Diagram)



Project Outcome / Deliverables

The expected outcome is a highly accurate, AI-driven phishing detection system capable of identifying and preventing phishing attacks in real time. It will efficiently distinguish between phishing and legitimate websites or emails with high precision and recall, minimising false positives and false negatives for enhanced cybersecurity. Furthermore, the system is expected to provide comprehensive logging and reporting capabilities for security analysis and incident response. Its modular design should facilitate future updates and integration of new detection techniques. Ultimately, this project aims to deliver a robust and scalable solution that significantly reduces the risk and impact of phishing attacks.

Assumptions

1. **Availability of a Labeled Dataset:** It is assumed that a reliable, pre-labeled dataset of phishing and legitimate URLs/emails is available for training and testing the model.
2. **Real-Time Detection Is Not Mandatory:** The system is designed for offline or batch processing; real-time constraints are not considered in this phase.
3. **No Privacy or Legal Constraints:** There are no ethical or legal limitations on the use of the dataset, as it is assumed to be open-source or publicly available.

References

1. ***Phishing Basics****: Nina Godbole and Sunita Belapure (2022). Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives. Wiley India pvt. Ltd., New Delhi. Pp. 570.*
2. ***Machine Learning****: Percy Vaughn(2023). Essentials of Machine learning. Larsen & Keller. Pp. 231*
3. ***Dataset*** *-https://data.mendeley.com/datasets/6tm2d6sz7p/1*