Recommendation from eLA

Hi Thang

Concerning Part A, Project Overview, and Client Requirements: It's essential to grasp the assignment specifications by thoroughly reviewing the assignment details on Canvas to ensure a comprehensive understanding of the requirements. These requirements entail

The first step is to define what malicious emails are and classify them based on pre-defined criteria.

Analyse the collected data to identify the general characteristics of malicious emails,

Implement the detection model using ML/DL algorithms.

The overall outcome and mark of the project will depend on the level of innovation and novel ideas included in the project, which is evaluated on two levels:

A new perspective on the common features of malicious emails

How the new detection system can overcome the deficiencies of existing detection systems

Hence, the suggestion I propose depends on your preference: you may choose to adopt a research methodology rooted in previous literature reviews to pinpoint gaps, gather relevant data, and scrutinize existing research to formulate and refine hypotheses. Alternatively, you could explore a case study methodology, examining real-world scenarios or instances to probe and authenticate hypotheses through meticulous analysis and comparison.

Executive summary

Coming soon . . .

Note: highlights are from my personally and also citied from Assignment criteria on Canvas. Anyone welcome to update for better quality for the purpose of better grade. Thanks.

Part A

Requirements from this part: Insightfully interprets information; identifies obvious as well as hidden assumptions clearly. Establishes the credibility of sources on points other than authority alone. From my perspective, in the client requirements, we need to provide credibility of sources on points other than authority alone. [remove this note after done this section]

Project overview:

Objective:

The project aims to assist individuals and enterprises globally in identifying and classifying malicious emails. Additionally, it involves analyzing collected data to uncover the common characteristics of such emails. Finally, the project report will recommend cutting-edge algorithms that leverage Machine Learning and AI to effectively filter out malicious emails and enhance user security.

Scope:

The report does not propose new algorithms or endorse purchasing tools from the market for filtering out malicious emails. Instead, it relies on information cited from recent articles, which will be listed in the preferences section below.

Client requirements:

According to our discussions and perspective, we assume that most clients expect their products to consistently meet the following categories

* Accuracy
* The new algorithms need to achieve high accuracy in identifying malicious emails for comparison with previous algorithms while also minimizing false positives to prevent legitimate emails from being incorrectly flagged as malicious.
* Reporting and Alerts:
* Create an intuitive interface that generates comprehensive reports on identified malicious emails and promptly alerts administrators or end-users when suspicious emails are detected.
* Real-Time Scanning
* Productivity and Effectively in terms of detection and response are critical.
* Scalability and Infrastructure
* The new algorithms ability to handle a large volume of incoming emails efficiently and considered to future growth.
* Ensure seamless integration with the client’s existing email servers or clients.
* Customizable Rules and Performance metrics
* Empower the client to establish personalized rules for email classification such as according to keywords, sender reputation, attachment types, etc.
* Consistently assess and provide updates on system performance
* Privacy
* Safeguard user privacy during the analysis of email content.

Part B

Individual need to do a design concept (please see the attached file in terms of classify malicious emails). Each teammate needs to choose one type of malicious email and to develop a potential design concept. (recommendation from eLA would be great hints for us)

Design concept: We used GitHub platform such as a repository to share documents, scripts between team members.

Such as A comprehensive description of three design ideas. An excellent rationale for design solutions with virtual architecture and design, and with an excellent relationship to stakeholder requirements.

More to come . . . .

Design concept 1:

Preliminary design:

* Methodology: Detail the approach and methodologies employed in the design process.

A clear description of design methodology for three design solutions that retain essential characteristics of the design problem. [remove this note after done this section]

* Design constraints: Thoroughly define the design constraints that influence the development of this particular design concept.

List of two or three different design constraints and specifications that are aligned with goal, scope, and context of the project. [remove this note after done this section]

* Specifications: Outline the technical specifications and requirements specific to this design concept.
* Vulnerability analysis: Conduct an analysis of potential vulnerabilities in the design and discuss measures to address them.

Justification of design:

Each team mate needs to do this part according to your design concept

Innovating concept provided. The concept is new and logical and draws upon analysis and research. Justifies two or three different designs with valid discussion.

In this section, from my perspective, we can express a new algorithm to do better job than existing algorithms like . . . . using machine learning (how ? and read articles to get more hints), if you have better ideas please go ahead. [remove this note after done this section]

Recommendation and conclusion

Coming soon. . .

References

1. <https://www.cyber.gov.au/protect-yourself/securing-your-email/email-security/protect-yourself-malicious-email>