Key Points

- It seems likely that the document "Research-Method-Activity-2-PROBLEM-FORMATION-RRL.pdf" contains a few errors that need correction for clarity and professionalism.
- Research suggests there are typos, capitalization inconsistencies, and phrasing issues in the problem statement, root cause analysis, and claims table.
- The evidence leans toward needing corrections like changing "hyperplanes" to "hyperlinks" and standardizing "phishing" to lowercase in several sections.

Document Overview

The document is a research method activity titled "Workshop on Problem Formulation & RRL," focusing on optimizing hybrid machine learning for phishing detection with improved URL and hyperlink analysis. It is authored by Nethan Bagasbas, Marco Licayan, Allen Vincent Roldan, and John Aaron Sabio. The content is divided into parts, including a problem statement, root cause analysis, literature map, claims table, and references, supported by recent studies from 2022 to 2025.

Identified Errors

After a detailed review, the following errors were found:

- **Typo in Root Cause Analysis:** The term "hyperplanes" appears in the root cause section, which should be corrected to "hyperlinks" for accuracy, as it relates to phishing detection involving URLs and hyperlinks.
- **Capitalization Inconsistencies:** The term "Phishing" is capitalized in several places where it should be lowercase, such as in the problem statement ("Phishing attacks" should be "phishing attacks") and root cause ("Phishing emails" should be "phishing emails"). This inconsistency affects professionalism and standard English usage.
- **Poor Phrasing in Claims Table:** The first claim title, "Enhanced Feature and Extraction as well as improving Detection Accuracy," is awkwardly phrased. It is recommended to revise it to "Enhanced Feature Extraction and Improved Detection Accuracy" for clarity.
- **Additional Capitalization Errors in Claims Table:** In the conclusions, "Phishing attempts" and "Phishing tactics" should be "phishing attempts" and "phishing tactics" respectively, to maintain consistency with standard lowercase usage.

Recommendations

To enhance the document's quality, the following corrections are suggested:

- Replace "hyperplanes" with "hyperlinks" in the root cause section.
- Ensure "phishing" is lowercase in all instances within sentences, correcting "Phishing" in the problem statement, root cause, and claims table conclusions.
- Revise the first claim title in the claims table for better clarity and grammatical flow.

These changes will improve the document's accuracy, consistency, and readability, making it more suitable for academic or professional use.

Detailed Survey Note

The document under review, titled "Research-Method-Activity-2-PROBLEM-FORMATION-RRL.pdf," is a research method activity focused on "Optimizing Hybrid Machine Learning for Phishing Detection with Improved URL and Hyperlink Analysis." Authored by Nethan Bagasbas, Marco Licayan, Allen Vincent Roldan, and John Aaron Sabio, it is structured into several key sections, including a problem statement, root cause analysis, literature map, claims table, and references, with citations from studies dated 2022 to 2025. This note provides a comprehensive analysis of the document, identifying errors and offering recommendations for improvement, ensuring it meets academic and professional standards.

Document Structure and Content

The document begins with an introductory section listing the title, "Workshop on Problem Formulation & RRL," and the members involved:

- Bagasbas, Nethan
- Licayan, Marco
- Roldan, Allen Vincent
- Sabio, John Aaron

This is followed by Part A, which includes the problem statement and root cause analysis using the "5 Whys" method, and a literature map visualized in Figure 2. Part B contains the claims table, outlining specific research claims and objectives. The document concludes with a list of 10 references, covering topics like phishing detection, machine learning, and deep learning approaches.

Detailed Error Analysis

Upon reviewing the document, several errors were identified, categorized as follows:

1. Typographical Errors

- **Location:** Root Cause Analysis section
- **Issue:** The term "hyperplanes" is used in the sentence, "Phishing emails and hyperplanes have become nearly indistinguishable from legitimate ones, causing machine learning models to struggle with accurate classification."
- **Analysis:** Given the context of the document, which focuses on URL and hyperlink analysis for phishing detection, "hyperplanes" is likely a typo for "hyperlinks." Hyperplanes are more relevant to machine learning classification boundaries, not phishing detection, making this an error.
- **Recommendation:** Change "hyperplanes" to "hyperlinks" to align with the document's focus.

2. Capitalization Inconsistencies

- **Locations:**
  - Problem Statement: "Machine learning models struggle to accurately classify Phishing attacks due to limited feature extraction and adaptability to emerging threats."
  - Root Cause: "Phishing emails and hyperplanes have become nearly indistinguishable from legitimate ones, causing machine learning models to struggle with accurate classification."
- **Issue:** The term "Phishing" is capitalized in both instances, which is inconsistent with standard English usage. In sentences, "phishing" should be lowercase unless it is part of a title or at the beginning of a sentence.
- **Analysis:** The area of study title, "Optimizing Hybrid Machine Learning for Phishing Detection with Improved URL and Hyperlink Analysis," correctly capitalizes "Phishing" as part of a title. However, within the body, "phishing attacks" and "phishing emails" should be lowercase for consistency and correctness.
- **Recommendation:** Change "Phishing attacks" to "phishing attacks" in the problem statement and "Phishing emails" to "phishing emails" in the root cause.

3. Claims Table Errors

The claims table, presented below, contains additional errors:

CLAIMS	MEASURE	SPECIFIC OBJECTIVE	CONCLUSION
Enhanced Feature and Extraction as well as improving Detection Accuracy	Precision, recall, and F1-score	Implement and fine-tune existing feature extraction techniques for URL and Hyperlink analysis	Improved accuracy in identifying Phishing attempts
Reducing False Positives and Increasing Detection Accuracy	False positive rate and Inaccuracies	Adjust classification models and apply filtering techniques to minimize false alarms	Reduced false positives and Increased detection accuracy
Implementing Real-Time Adaptive Learning Mechanisms for Effective Detection of evolving Phishing tactics	Adaptation rate and detection speed	Utilize pre-existing libraries for continuous learning and integrate with threat intelligence feeds	Improved adaptability to emerging Phishing tactics

- **Issue 1: Phrasing in First Claim Title**
  - Current: "Enhanced Feature and Extraction as well as improving Detection Accuracy"
  - Analysis: This phrasing is awkward and unclear. It seems to combine two ideas, "Enhanced Feature and Extraction" and "improving Detection Accuracy," but "Feature and Extraction" is likely meant to be "Feature Extraction." The current form is grammatically incorrect and confusing.

    - Recommendation: Revise to "Enhanced Feature Extraction and Improved Detection Accuracy" for clarity and correctness.

- **Issue 2: Capitalization in Conclusions**
    - Locations:
        - First claim conclusion: "Improved accuracy in identifying Phishing attempts"
        - Third claim conclusion: "Improved adaptability to emerging Phishing tactics"
    - Analysis: Similar to the problem statement, "Phishing" is capitalized here, which is incorrect for sentence-level usage. It should be "phishing attempts" and "phishing tactics" respectively.
    - Recommendation: Change "Phishing attempts" to "phishing attempts" and "Phishing tactics" to "phishing tactics."

4. Additional Observations

- The literature map and root cause analysis sections reference figures (Figure 1 and Figure 2), but the detailed content of these figures was not accessible for review. Based on the descriptions provided, no textual errors were identified in these sections, but visual elements could not be verified.
- The references section, listing 10 studies, appears correctly formatted with DOIs and publication details, and no errors were found in author names, titles, or citations.

Recommendations for Improvement

To enhance the document's quality and ensure it meets academic standards, the following actions are recommended:

1. **Correct Typographical Errors:** Replace "hyperplanes" with "hyperlinks" in the root cause section to align with the document's focus on URL and hyperlink analysis.
2. **Standardize Capitalization:** Ensure "phishing" is lowercase in all sentence-level usage, correcting instances in the problem statement, root cause, and claims table conclusions as outlined.
3. **Improve Phrasing:** Revise the first claim title in the claims table to "Enhanced Feature Extraction and Improved Detection Accuracy" for clarity and grammatical correctness.
4. **Review Visual Elements:** Although figures could not be reviewed, ensure that Figure 1 (Root Cause Analysis) and Figure 2 (Literature Map) are consistent with the textual descriptions and free of errors, if possible.

Conclusion

This review highlights the importance of attention to detail in academic documents, particularly in ensuring typographical accuracy, consistent capitalization, and clear phrasing. By implementing the recommended corrections, the document will be more professional, readable, and aligned with standard English usage, enhancing its suitability for research purposes.

Key Citations

- Staying Ahead of Phishers: A Review of Recent Advances and Emerging Methodologies in Phishing Detection
- [AI for Phishing Detection: Using Pattern Recognition and Real-Time Analysis to Identify Threats] (no URL provided in text)
- PhishSim: Aiding Phishing Website Detection With a Feature-Free Tool
- Evasion Attacks and Defense Mechanisms for Machine Learning-Based Web Phishing Classifiers
- [Phishing Website Detection Using Machine Learning: A Review](no URL provided in text, Wasit Journal reference)
- Modeling Hybrid Feature-Based Phishing Websites Detection Using Machine Learning Techniques
- A Case Study on Phishing Detection With a Machine Learning Net
- A Deep Learning-Based Framework for Phishing Website Detection
- Web-based phishing URL detection model using deep learning optimization techniques
- Characteristics of Understanding URLs and Domain Names Features: The Detection of Phishing Websites With Machine Learning Methods