Republic of the Philippines
CAVITE STATE UNIVERSITY
Don Severino de las Alas Campus
Indang, Cavite

A Machine Learning-Based Cyber Threat Detection System for Network Security~~RESEARCH PROPOSAL TITLE~~

Rationale/ Introduction

With the rise of cyber threats, traditional rule-based security systems struggle to detect sophisticated attacks such as zero-day exploits and advanced persistent threats (APTs). Machine learning (ML) has emerged as a powerful tool in cybersecurity, enabling automated threat detection through pattern recognition and anomaly detection. By analyzing network traffic, ML models can identify suspicious behaviors in real-time, helping organizations prevent security breaches before they escalate. This research aims to develop a machine learning-based cyber threat detection system that enhances network security by improving threat identification accuracy and reducing false positives. ~~<Insert content; In-text citations are needed>~~

Significance of the Study

This study is significant as it explores the role of machine learning in strengthening cybersecurity defenses. By developing an ML-powered cyber threat detection system, this research will contribute to automated security monitoring, benefiting network administrators, IT security teams, and organizations seeking to enhance their defenses against cyber attacks. The findings will provide insights into improving real-time threat detection, reducing human intervention in security monitoring, and addressing limitations such as adversarial attacks and model biases. ~~<Insert content>~~

Scope and Limitations of the Study

This study will focus on developing and evaluating a machine learning-based threat detection system for identifying anomalies and suspicious activities in network traffic. It will assess the system's effectiveness in detecting various cyber threats, such as malware, phishing, and intrusion attempts. However, the study will not cover other cybersecurity

Formatted: Font: Bold
Formatted: Centered
Formatted: Font: (Default) Arial, Bold
Commented [1]: Put your tentative thesis title here.
Remember:
A4 size, Arial 11
Academic Writing Style (good writing style should be considered)
APA formatting (referencing and in-text citation)
Always make sure that your proposal falls under any 3 prioritized CS research tracks
Avoid plagiarism
Always make sure that your proposed study is specific and attainable.
Formatted: Font: (Default) Arial
Commented [2]: Yung Rationale po ay nageexplain the reason behind your proposal - why do you propose that research idea.
First paragraph: Introduce ano yung problem or yung research gap. It is something that you want to address. Not because it is called problem ay direct problem na ito. It can be the gap, weaknesses, issues, or based on recommendations from existing literature.

Second paragraph: In few sentences, describe how you'll be able to solve the research gap or isolve ang weaknesses nito.

Third paragraph: Potential impact. Dito nyo na ihighlight yung expected outcomes or benefits nito.

Fourth paragraph: Conclusion. Just a summary of this rationale and conviction na maipush ang proposal nyo. This highlights yung value ng proposal nyo to contribute sa field ng CS.

NOTE: ACADEMIC WRITING STYLE should be followed. No to ChatGPT :)
Formatted: Justified, Indent: First line: 1.27 cm
Formatted: Font: (Default) Arial
Commented [3]: Itong section na ito ay nageexplain bakit yung study ay dapat at worth gawin, at kung bakit yung magiging findings mo dito ay mahalaga at makabuluhan. May magiging impact ba ito in the future? Pwede ba itong magamit sa iba't ibang field for them to develop their own technologies, etc.

Dito rin dapat ilagay yung "possible" contribution nito sa U.N. SDG. Basahin po muna ang https://www.un.org/sustainabledevelopment/sustainable-development-goals/ bago maglagay ng content. Wag magassume dahil may focus ang bawat goal.

Dito rin ilagay po ang involvement ng proposal nyo sa CvSU Thematic Area. If one or more involved areas, okay lang po basta maijujustify nyo po sa section na ito.
Formatted: Justified, Indent: First line: 1.27 cm
Formatted: Font: (Default) Arial
Formatted: Justified, Indent: First line: 1.27 cm

aspects, such as encryption methods or legal frameworks, nor will it focus on threats originating from insider attacks.

Formatted: Indent: First line: 1.27 cm

Objectives of the Study

This study aims to design and develop a machine learning-based cyber threat detection system to improve network security. By evaluating its accuracy, efficiency, and scalability, the research seeks to enhance automated cybersecurity solutions. Specifically, it will:

1. Develop a machine learning model capable of detecting cyber threats in network traffic.
2. Evaluate the system's accuracy and efficiency in identifying security threats compared to traditional detection methods.
3. Identify challenges and propose improvements for machine learning-based cybersecurity solutions.

Expected Outputs

Expected Outputs

The research is expected to produce a functional machine learning-based cyber threat detection system prototype. It will provide an analysis of the system's effectiveness in detecting threats, minimizing false positives, and enhancing network security. Additionally, the study will offer recommendations for optimizing ML-powered security systems and addressing challenges such as data quality, adversarial attacks, and computational costs.

Commented [5]: Imagine na yung inyong proposal po ay nagmamaterialize na. You need to identify ano yung mga features, sub-routines, or functions na maicocover po ng inyong study. If experiments, describe how the experiments will worl then ano yung possible or expected output from it.

Description of outputs (specifications, datasets, algorithms, prototypes, etc.)
Description of materials to use

Formatted: Justified, Indent: First line: 1.27 cm

References

Buczak, A. L., & Guven, E. (2016). *A survey of data mining and machine learning methods for cyber security intrusion detection*. *IEEE Communications Surveys & Tutorials, 18*(2), 1153-1176.

Commented [6]: Use legit materials po. Use APA formatting

Lippmann, R. P., Fried, D. J., Graf, I., Haines, J. W., Kendall, K. R., McClung, D., ... & Zissman, M. A. (2000). *Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation*. *Proceedings of the DARPA Information Survivability Conference and Exposition, 2*, 12-26.

Sommer, R., & Paxson, V. (2010). *Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy*, 305-316.