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

AI-Powered Malware Detection System Using Deep Learning
~~RESEARCH PROPOSAL TITLE~~

Rationale/ Introduction

As cyber threats continue to evolve, traditional signature-based malware detection methods struggle to keep up with new and sophisticated attacks. Conventional antivirus software relies on predefined malware signatures, making it ineffective against zero-day exploits and polymorphic malware. Deep learning, a subset of artificial intelligence (AI), has shown promise in cybersecurity by enabling automated threat detection through pattern recognition and anomaly detection. This research aims to develop an AI-powered malware detection system that utilizes deep learning techniques to identify malicious activities in real time. The study will evaluate the accuracy, efficiency, and adaptability of AI-driven approaches in detecting previously unknown malware variants. ~~<Insert content; In-text citations are needed>~~

Significance of the Study

This study is significant as it explores the use of AI in enhancing cybersecurity by providing a proactive malware detection approach. By developing a deep learning-based detection system, this research will contribute to automated threat identification, benefiting cybersecurity experts, organizations, and individuals. The findings will provide insights into the effectiveness of AI in combating advanced malware threats while addressing challenges such as false positives, computational overhead, and adversarial attacks designed to evade detection. Additionally, the study will examine the ethical implications and practical considerations of deploying AI in cybersecurity. ~~<Insert content>~~

Scope and Limitations of the Study

This study will focus on designing and testing an AI-powered malware detection system using deep learning algorithms. It will assess the system's ability to detect and classify various malware types, including ransomware, trojans, and spyware. However, the study will

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: Centered

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: Font: (Default) Arial

Formatted: Justified, Indent: First line: 1.27 cm not cover other cybersecurity measures such as network firewalls, intrusion prevention systems, or manual malware analysis techniques.

Formatted: Indent: First line: 1.27 cm

Objectives of the Study

This research aims to develop an AI-driven malware detection system that improves real-time identification and classification of cyber threats. By analyzing its accuracy and adaptability, the study seeks to enhance automated security solutions.

Specifically, it will:

1. Develop a deep learning-based malware detection system capable of identifying known and unknown threats.
2. Evaluate the system's accuracy, efficiency, and false positive rate compared to traditional detection methods.
3. Identify challenges and propose solutions for optimizing AI-powered malware detection in real-world applications.

Expected Outputs

Expected Outputs

Formatted: Font: 11 pt

The research is expected to produce a prototype AI-powered malware detection system that improves accuracy and response time in cybersecurity. Findings will include a comparative analysis of AI-based detection versus traditional signature-based methods, as well as recommendations for integrating deep learning into cybersecurity frameworks. Additionally, the study will highlight potential improvements and limitations, such as adversarial resistance and scalability concerns.

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.

Kolosnjaji, B., Zarras, A., Webster, G., & Eckert, C. (2018). *Deep learning for classification of malware system call sequences. Neural Networks, 100*, 19-38.

Saxe, J., & Berlin, K. (2015). *Deep neural network-based malware detection using two-dimensional binary program features. Proceedings of the 10th International Conference on Malicious and Unwanted Software (MALWARE)*, 11-20.

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

Formatted: Justified, Indent: Left: 0 cm, Hanging: 1.27 cm