Aaron Tsatsu Tamakloe

Ashesi University

SOAN325: Research Methods

Final Written Report | Computer Science Thesis Capstone

Prof. Eric Acheampong

Prof. Gideon Hosu-Porbley

December 6, 2023.

ABSTRACT

In recent years, the proliferation of malicious software, or malware, has posed a significant threat to the security of computer systems. Unfortunately, newer trends of these malware render conventional signature and heuristic-based approaches inefficient for detecting malware. Hence, a machine-learning approach to detecting malware is a clever solution. This paper delves into a comprehensive analysis of various machine-learning techniques for detecting malware. This study explores various machine-learning model development layers, including algorithm selection, feature engineering and evaluation methodologies. By investigating the advantages of various machine learning models, encompassing model-merge or ensemble techniques, the study aims to uncover which strategies are most adept at detecting new malware variants. In summary, the research will present that a machine-learning-based proof-of-concept could effectively detect existing malware and its newer variants.

Keywords: malware, malware detection, machine learning, feature selection, algorithm selection

Contents

CHAPTER 1: INTRODUCTION

1.1 BACKGROUND

Malware is malicious software disseminated to infiltrate a system's secrecy, integrity, and functionality, such as viruses, worms, trojans, and spyware. (Hardy et al., 2016). As the world evolves technologically with a dominant adoption of mobile devices, malware attacks skyrocket. Generally, other software or human error can initiate malware attacks. According to Lévesque et al. (2018), most vulnerabilities occur after cyber attackers have enticed users to perform basic tasks like opening email attachments or visiting a malicious website. This little yet significant cause of malware spread necessitates sophisticated techniques to mitigate malware invasion.

Over the years, several approaches for detecting malware have emerged. Examples of these approaches, which research now considers traditional techniques, include the manual heuristic and signature matching-based methods. As mentioned earlier about the various types of malware, the traditional approaches use the distinct features of the malware types to detect malware. The drawback with these conventional approaches is that they fail dramatically at detecting unknown malware as newer variants present themselves with a culmination of the various malware qualities. (Aslan & Samet, 2020). An alarming perspective of malware attacks is their heavy impact on global economies. In 2020, the overall economic cost of cybercrime in the USA was estimated at US$ 1tillion. (Eling et al., 2022).

A promising solution to the current inefficient malware detection techniques is a machine-learning-based one. Machine learning approaches leverage the power of artificial intelligence and data-driven insights to detect subtle patterns and anomalies in software behaviour, enabling the identification of previously unknown malware strains. Researchers have discovered several machine learning models that can detect malware with some decent accuracy compared to

conventional methods. However, none of these researchers have conclusively declared that one model is more effective than all existing models. The reason is that each model presents its drawbacks and benefits. This explains how uneasy it is to develop a one-model-fits-all solution and the essence of further research. This paper seeks to comprehensively explore the existing machine learning models by carefully identifying the impact of feature engineering, algorithm selection and ensemble techniques on the efficiency of the models in detecting malware.

1.2 PROBLEM STATEMENT

The world's increasing reliance on computer systems for streamlining everyday tedious activities like shopping, transferring documents, etcetera poses a critical problem via the exposure to malware vulnerabilities. According to the International Business Machines Corporation, 95% of cyber security breaches in 2022 resulted from human error. While researchers have employed manual malware detection strategies with varying degrees of success, the increasing complexity of malware trends necessitates a paradigm shift in malware detection. This paper's research on the machine learning paradigm shift in malware detection will explore and analyze several machine learning models to identify the most adept in detecting previously unknown malware.

1.3 PURPOSE/OBJECTIVE

The primary purpose of this study is to evaluate the efficiency of various machine-learning-based malware detection approaches based on their accuracy levels and other efficiency metrics, such as how responsive they are to new malware variants.

Main Objective:

i. To evaluate the effectiveness of machine learning techniques in detecting malware, specifically focusing on their capability to identify evolving malware variants.

Subobjective:

i. To examine the impact of algorithm selection on machine-learning-driven malware detection models.

ii. To evaluate the significance of ensemble techniques on machine-learning-driven malware detection models.

1.4 HYPOTHESES/RESEARCH QUESTIONS

Hypothesis:

Unlike conventional signature and heuristic-based approaches, machine-learning-driven approaches in malware detection will positively affect the accuracy of new malware variant detection in computer systems.

Some questions that this study seeks to answer include:

i. What is the effect of machine learning techniques on evolving-malware detection?

ii. How do ensemble techniques impact the malware detection capabilities of machine learning models?

iii. How do machine learning models compare differently in their ability to detect unknown malware strains accurately?

1.5 SIGNIFICANCE OF STUDY

As noted earlier, the high rise in varying strains of cyberattacks as the world evolves technologically is critical. The significance of this study lies in its potential to revolutionize computer systems security by leveraging the powerful capabilities of machine learning while curtailing unavoidable human error as a cause of malware spread and saving the world economy billions of dollars.

CHAPTER 2: LITERATURE REVIEW

The relentless evolution of malicious software (malware) necessitates innovative approaches to enhance the security of computer systems. In response to this persistent need, several researchers have increasingly explored the dynamic field of machine learning to reinforce malware detection capabilities. Before reviewing the current literature, this paper situates the research in the context of relevant theories like resilience and decision theories. The paper also operationalizes critical variables within the research. These form the theoretical and conceptual framework of the research. This literature review seeks to present a nuanced exploration of the current malware detection landscape given a machine learning background by examining the types of machine learning algorithms currently employed by researchers, their applications, challenges these approaches have encountered, and the innovations that have reshaped the malware detection field in recent years.

2.1 REVIEW OF CONCEPTUAL/THEORETICAL LITERATURE

2.1.1 Conceptual Framework

This study's conceptual framework is structured around evaluating the efficiency of various machine learning-driven approaches for malware detection, explicitly focusing on their accuracy in identifying evolving malware variants. The critical variables in the research are: 1) the machine learning techniques employed, 2) the impact of algorithm selection, 3) the significance of ensemble techniques, and 4) the overall effectiveness of the machine learning models in detecting new malware strains.

Drawing from Saad et al. (2019b) and Kimmel et al. (2021), the selection of machine learning techniques like k-Nearest Neighbour, Naïve Bayes, and ensemble techniques influenced

their demonstrated efficacy in malware detection. Also, Firdausi et al. (2010) provide insights into the impact of algorithm selection on the accuracy of malware detection models, guiding the research in considering the relevance of algorithmic decisions. Lastly, leveraging the work of ensemble techniques, Kimmel et al. (2021) acknowledge the effectiveness of combining multiple algorithms to enhance malware detection capabilities. These three mentioned variables form the independent variables for the study. Regarding dependent variables, the research considers the accuracy in detecting evolving malware variants dependent on the machine learning techniques used.

Furthermore, with existing research like those by Firdausi (2010), the efficiency metrics outlined for the machine learning models form the mediating variables of the study. Some of these metrics include precision and recall. Finally, considering the dynamic nature of malware, insights from Kimmel et al. (2021) inform the inclusion of malware characteristics as moderating variables, acknowledging the potential impact on the performance of machine learning models. With the careful selection of these variables based on the work of other researchers, the study hypothesizes that the careful selection of machine learning techniques, algorithmic decisions and the integration of ensemble methods will positively influence the accuracy of detecting new malware variants, considering the moderating influence of different malware qualities.

2.1.2 Theoretical Framework

Resilience Theory

The resilience theory concerns systems' capacity to withstand and bounce back from disruptions. According to Breda (2018), resilience deals with the tenacity that builds up (mostly among people, but in this paper's context, systems) from the ability to surmount adversities and

stressors. The theory evolved from traditional disaster recovery to adaptability and robustness. The resilience theory has been used previously in several respects, including resilience in families, communities, workplaces, and among individuals. A relevant context within which the theory has been employed is in cybersecurity resilience, which is the foundation on which this paper's study is developed. The theory has seen significant contributions from cybersecurity resilience researchers like Daniel Geer.

Resilience theory is helpful in this paper's research as it helps to examine the resilience of machine learning-driven malware detection systems, especially while considering evolving malware variants and adversarial attacks. By situating the research within the resilient theory, the paper will explore how current and proposed systems can adapt to changing conditions in malware attacks.

Decision Theory

The decision theory is concerned with choosing between some given optional courses of action when the repercussions associated with that choice or option are partially known. (North, 1968). Decision theory has evolved from foundational principles of rational decision-making to uncertainty considerations. The theory has been used extensively in domains like mathematics and machine learning. The theory, contributed to by decision theorists like Leonard Savage and other machine learning researchers, is highly relevant to this paper's work of detecting malware based on specific rules or data previously trained on a machine learning model. With lots of uncertainty about the evolving malware variants, the outcome of the research should effectively provide a framework for making logical decisions that can detect malware. The decision theory in this research explores how machine learning algorithms can make decisions while detecting malware,

considering the unknowns of malware types and potential consequences like false positives and false negatives.

This research hinges on several technical computer science concepts to explain the problem. In this paper's review of current literature around malware detection using machine learning, these concepts are extensively employed to effectively discuss the findings from existing research and the prospects of this research. In this section, the paper highlights the operational definitions of the variables involved in this study. That is, machine learning (ML), malware, malware variants or strains, deep learning, accuracy as a performance metric and ensemble techniques. According to Naqa et al. (2015), machine learning is a "branch of computational algorithms designed to emulate human intelligence by learning from the surrounding environment." In the context of this research, machine learning "learns" different types of malware and tries to detect them intelligently, as a cybersecurity expert would have done less efficiently.

Due to the evolving manner of the field, researchers have adapted a term called traditional machine learning models, which were the foundational models on which the field has evolved. Examples of these models include the Support Vector Machine, k-nearest Neighbors, Random Forest and Regression analysis. An improvement to machine learning is what has become deep learning. LeCun et al. (2015) explain this field as a computational model comprising several processing layers to learn data representations with several abstraction levels. Examples of this paradigm are Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Generative Adversarial Networks. Throughout the review, these models yield themselves to be more highly performing than the traditional models. A common way in which the performance of these models is measured, especially in this paper's study, is the accuracy metric. Accuracy is the percentage of correct classifications a trained machine learning model gets. Finally, in the context

of this research, ensemble techniques are approaches to solving problems by combining several machine learning and deep learning algorithms to enhance performance.

Another relevant concept for this research is malicious software (contracted as malware). Malware is software that is designed to cause harm to a computer system intentionally. (Ngo et al., 2020) In the context of this paper, several malware types exist. These types are called malware variants or strains, meaning new types of malware previously appearing in a form that has not been seen (mainly by a machine learning algorithm).

2.2 REVIEW OF EMPIRICAL LITERATURE

Types of Machine Learning Algorithms for Malware Detection

Within the expansive machine learning domain, various algorithms have been developed to confront computer system vulnerabilities or malware in general. The need to employ machine learning techniques – dynamic malware detection approaches – has grown exponentially due to the current challenge of systems' inability to detect malware variants accurately. The significance of dynamic malware techniques is for the efficient discovery of unconventional malware that malware detection systems have not previously encountered. Cybersecurity experts have confidently asserted that artificial intelligence and machine learning-driven systems will remedy modern malware vulnerabilities. (Saad et al., 2019b). As evidence of Saad et al.'s assertion, researchers like Kimmel et al. (2021) and Firdausi et al. (2010) conducted experiments on some machine learning algorithms like the k-Nearest Neighbor, Naïve Bayes, Support Vector Machine and the J48 decision tree classifier algorithms, with different levels of accuracy.

After collecting several malware samples and setting up a virtual environment to run experiments on the various machine-learning classification algorithms, Firdausi et al. (2010)

conducted 220 tests. The experiment was such that malware was strategically injected into the virtual environment to ensure the results reflected the detection algorithms. Using the accuracy levels as a performance metric, the experiment showed 92.9%, 65.4%, 91.7%, 94.9% and 94.2% for the k-Nearest Neighbor, Naïve Bayes, Support Vector Machine, J48 decision tree and Multilayer Perceptron neural network, respectively. These experiment results prove that the J48 decision tree is the best performing in malware detection among the traditional machine learning classification algorithms. However, the fast-evolving nature of the machine learning domain has caused a quick challenge to the results of Firdausi et al. (2010).

Kimmel et al. (2021) conducted a similar study, which did not only include the traditional machine learning classification algorithms but also an additional algorithm called the Convolutional Neural Network. As with Firdausi et al. (2010) study that considered the algorithms' accuracy as a performance level, Kimmel et al. (2021) employed a similar metric which resulted in 92.9%, 87.56%,89.36%, 72.34%, 81.47% and 58.09% for the Convolutional Neural Network (CNN), Support Vector Classifier, Random Forest Classifier, k-Nearest Neighbor, Gradient Boosted Tree and the Gaussian Naïve Bayes, respectively. This result implies that the traditional machine learning algorithms are currently not up to task to detect malware. Hence, due to its high performance, the Convolutional Neural Network (CNN) is the ideal machine learning algorithm to detect malware. A logical explanation for such challenging results is the dynamic nature of the machine learning domain over the years. To situate this paper's work in the current approaches and their results, a traditional machine learning classification algorithm cannot be used to detect malware variants. However, whether the CNN algorithm can detect malware variants remains, which is the fundamental problem this paper seeks to address. As expected, some researchers have criticized the CNN algorithm for being constrained by the data size used to train the model. In their

recent survey, Tayyab et al. (2022) mention several other deep learning algorithms which can be complementary to CNN to achieve better results. These findings are, however, discussed later in the innovations and advancement section of this review.

Applications and Effectiveness

The practical deployment of machine learning-driven malware detection approaches extends across all aspects of computing landscapes. From traditional computer systems to mobile devices and the fast-rising Internet of Things (IoT) and cloud computing realms, machine learning algorithms have proven high usability and adaptability. Researchers like Zhang et al. (2018), Sahs and Khan (2012), Gaurav et al. (2023), and Al-Hawawreh et al. (2018) have provided a paradigmatic illustration of this adaptability through fields like Android devices, IoT, cloud computing, etcetera. These applications are relevant to this study as they explore various computer systems and provide a comprehensive remedy for malware vulnerabilities. In the mobile devices realm, Sahs and Khan (2012) employed a feature extraction approach on packaged Android applications, which were later trained on a support vector machine classifier. The results of this application were entirely low rates of false negatives, which meant that the system had a low rate of tagging computer resources as not being malicious when they were malicious. The study by Sahs and Khan (2012) helps to revolutionize mobile devices and smartphones, which are easier targets for malware.

Another significant application of malware detection using machine learning approaches has been in the Industrial Internet of Things (IIoT) domain, which researchers like Al-Hawawreh et al. (2018b) have covered. Their study suggests an "anomaly detection system", which serves as a malware detection system in this review's context. The approach adopted in their research highlights the essence of deep learning, a much-sophisticated iteration of machine learning.

According to Al-Hawawreh et al. (2018b), the damages involved in sustaining vulnerabilities in the IIoT system will rise to about $90 trillion in 2030. This makes their anomaly detection system, which employs deep learning, a convenient and promising control remedy to these threats. It is paramount to note how all research conducted so far has extensively discussed the role of machine learning in detecting malware while highlighting its versatility in all fields. An exciting field that follows this trend is the Internet of Things (IoT) domain, which is closer to the everyday computer user than the earlier discussed IIoT.

The Internet of Things is a computer science field concerned with fascinating systems like smart homes and intelligent assistants. Considering the degree of technological control over a system like a smart home, which is supposed to be the private dwelling of users, it is highly vital to apply state-of-the-art technologies to combat any form of intrusions or malware vulnerabilities. This makes the research by Gaurav et al. (2023) relevant to this paper's study. Aside from its use of machine learning approaches, the primary approach this paper promotes, it captures the gap of current models' inability to effectively identify evolving malware or previously unseen malware variants. They achieve this by employing an adversarial detection model where data used to train the machine learning models include malicious samples to suppress the effectiveness of the model's training intentionally. From the findings discussed earlier in this review, a leaning towards Gaurav et al. (2023) adversarial approach, together with promising techniques like the Convolutional Neural Network or deep learning, in general, seems apt to achieve the objective of accurately detecting previously unseen malware.

Challenges and Vulnerabilities

As promising as machine learning approaches for detecting malware may be, it is essential to carefully analyze the general demerits and challenges they may pose to the security field. While

researchers have discussed the applications and significance of machine learning in malware detection, they have equally highlighted the issues associated with this ever-promising remedy. Some researchers, including Gibert et al. (2020c), have extensively discussed security researchers' issues. Paramount among the issues is the availability of public malware benchmarks for researchers. Unlike other fields, the cybersecurity field is internally constrained legally to publicly provide necessary data about malware, which can potentially enhance current research. As such, current research suggests solutions that may not necessarily cover all malware possibilities actively encountered in the industry or practical use cases for an everyday user. The challenge with this constraint is that it is nearly impossible to effectively compare performance metrics across different studies since each study employs its dataset.

Saad et al. (2019b) also highlight another challenge: the interpretability of malware detection systems using machine learning. Difficulty in providing meaningful explanations to the output of machine learning algorithms that detect malware defeats the purpose of knowing how to explain how effective the algorithm has been in detecting malware variants. Saad et al. (2019b) state that "interpreting machine learning models is a new and open challenge." A possible makeup for this "open challenge" is a potential domain-specific interpretation for machine learning remedies. That is, solutions in the cloud computing field will be different from those in the IoT domain. This poses a significant challenge to this research's primary objective: developing a machine-learning algorithm that detects malware in all computer systems. If interpretations of machine learning solutions must be domain-specific, this leaves an unhandled issue of making generic interpretations for all computer systems.

Innovations and Advancements

Among all the study results reviewed above as promising remedies to detecting malware by leveraging machine learning, some have stood out due to their innovative perspective and improvements on the promising approaches. Some of these approaches include ensemble techniques that create compositions of two or more accepted machine learning techniques, deep learning, and deep neural networks, all improving machine learning. Other approaches have also slightly adjusted Convolutional Neural Networks (CNN) to improve efficiency. Tayyab et al. (2022) highlight several approaches researchers have employed to detect malware. Deep learning approaches like Convolutional Neural Network and Recurrent Neural Network (RNN) are recurrent among the list. The relevance of such approaches to malware detection is that they revolutionize the ability of systems to amicably handle previously unseen malware variants, which is this paper's primary goal.

2.3 CONCLUSION

In conclusion, situating this paper's work in the context of existing literature outlines the dynamism present in state-of-the-art machine-learning approaches in detecting malware in computer systems. The discussion of the existing diverse machine learning algorithms, their applications, challenges, and innovations reveals the strides made in the field to tackle the problem in one way or another. The review's synthesis underscores the importance of innovative techniques to anticipate malware variants. This synthesis has since guided the path that this paper's research will chart by employing ensemble techniques and making room for all sorts of constraints that exist in detecting malware dynamically. Though not a finality, the review's synthesis has provided a comprehensive understanding of arrangements to make to fill the current research gap.

CHAPTER 3: METHODOLOGY

Introduction

The primary idea of this research is to determine, by an experimental approach, the most effective machine-learning strategies or approaches for detecting new malware variants. This research explores the ensemble paradigm and general deep learning models like the Convolutional Neural Networks (CNN) to help identify existing malware and newer variants that could bypass current security systems for preventing or handling malware attacks. In this section, the paper provides an overview of the research's approach to answering the research questions that seek to fill out the research gap identified earlier. The section also discusses a proposed way to conduct experiments while looking for provisional results and ways to validate the expected results from the experiment. Finally, the section summarises the research prospectus and potential future additions to the suggested work in this study.

3.1 METHODOLOGY

3.1.1 Rationale for Ensemble Techniques and Deep Learning

To answer the research questions posed by this study, the research employs ensemble techniques to harness the collective power of multiple machine learning models to enhance malware detection system robustness. From the review of existing literature, the paper found that individual machine-learning models had contributed some decent efficiency in detecting malware. While some researchers combined supervised machine learning models like the Random Rain Forest and Support Vector Machine models, deep learning models proved highly effective. Hence, this study combines deep learning models with traditional machine learning approaches to probe higher effectiveness that could revolutionize malware detection using machine learning.

3.1.2 Machine Learning Algorithms

The machine learning algorithms that this research seeks to employ can be categorized into two broad areas of study: 1) a combination of some traditional machine learning models and deep learning models and 2) an ensemble of deep learning techniques. From the literature review, the most promising traditional machine learning models in malware detection are the Support Vector Classifier, Random Forest Classifier and k-nearest Neighbor. The first categorization stated earlier will combine these three models with the Convolutional Neural Network (CNN) to investigate their effectiveness. The second categorization will involve piecing the CNN and Recurrent Neural Network (RNN) models. The relevance of the ensemble technique involving the traditional model will provide flexibility in handling diverse features of the input data, extracting temporal aspects of the data and considering the training data's hierarchical features. Consistent with this paper's introduction, feature selection is essential for effective malware detection.

3.1.3 Research Design and Data Collection

Researchers like Kamiri and Mariga (2021) have stated categorically that machine learning-focused research is primarily quantitative due to the involvement of numerical data and statistical techniques for analyzing the data, and this research is no different. This study employs a quantitative approach in its methods, specifically experimental design. This approach is because the data used for the study needs to be tested under various conditions to monitor their outputs and subsequently inform this study's findings. The scientific experimental approach will help test the hypotheses formulated earlier in the study and observe causal effects among the chosen variables.

Having diverse datasets has proven to be the fundamental driver of success for most existing research in the machine learning and malware detection domains. However, from the

findings of this paper, the cybersecurity industry is challenged with having standardized data to represent all the malware attacks unleashed on systems. Aside from that, there is hardly any available data for research purposes. As such, the best bet for this study is to employ secondary data. The dataset for this research will be sourced from reputable repositories employed by researchers like Sewak et al. (2018). The sources include datasets from the benchmark Malicia project (Sharma & Sahay, 2016) and benign instance datasets employed by Firdausi et al. (2010). After the data is collected, the following steps will be performed to ensure the data's integrity and preparedness for the experiment: 1) clean, prepare and manipulate data 2) train the machine learning models 3) test the data collected 4) make iterations to improve and validate the results. The data collected will be broken down into training, testing and validation subsets. 70% will be used for training, 20% will be used for testing, and 10% will be used for validation.

3.2 EXPERIMENTAL SETUP AND COMPUTATIONAL MODEL

3.2.1 Computer Environment

The study's experimental setup leverages a robust hardware infrastructure to handle the computational demands of complex machine learning and deep learning models' training. A high-performance computer will serve as the main framework for the experiment, comprising nodes equipped with Intel Xeon Scalable Processors and NVIDIA V100 Tensor Core Graphical Processing Units (GPUs). This configuration will ensure parallel processing capabilities, facilitating highly efficient training of the deep learning models.

3.2.2 Software Stack

For this research, the software stack employed is critical to the experiment's outcome. Hence, drawing from the highs and pitfalls of other researchers, this study carefully curates a comprehensive environment for implementing machine learning algorithms. The experiment will use version 3.12.0 of the Python Programming Language for this research, supported by essential Python libraries like NumPy, pandas, sci-kit-learn, TensorFlow and Keras.

3.2.3 Evaluation Metrics

Considering the complexity of the ensemble techniques employed in this study, the experiment requires a rigorous evaluation metric to assess the performance of the deep learning models and the ensemble techniques. Maintaining the standard machine learning approaches, the experiment will use the confusion matrix, which visualizes the ratios of true positives to false positives and that of false negatives to true negatives. Aside from these, the study will also employ the derivates of the confusion matrix, including the accuracy, recall, precision and F1 score of the trained models.

3.3 PRELIMINARY RESULTS

The prospective outcome of this study is promising. Ensemble models, integrating Random Forest and deep learning models, demonstrate robust performance and enhanced malware detection accuracy. The Convolution Neural Network (CNN) proves effective in capturing intricate spatial patterns, while the Recurrent Neural Networks (RNN) provides valuable insights into the temporal dependencies of the experiment. Some of these results are evidenced in the reviewed

literature. Considering the validation strategies the study will employ, the experiment's results can ensure stability and consistency, making it easier to generalize the results.

3.4 EXPLANATION OF THE REST OF THE WORK TO BE ACCOMPLISHED

The rest of the work to be accomplished in this research involves optimizing the ensemble models and deep learning techniques to mitigate overfitting concerns that could come up. That is, the trained models are working effectively on training data but not on new data. Aside from that, the study will attempt to address the interpretability challenge of malware detection models by exploring the use of dynamic environments to allow for the generalizability of results and more straightforward explanations for the behaviours of the models. Furthermore, the study will provide a comparative analysis of the research results vis-à-vis existing works and structure comprehensive documentation disseminating the experiment's findings.

3.5 VALIDATION METHODS OF EXPECTED RESULTS AND EXCEPTIONS

To effectively validate the expected results of this experiment and identify exceptions, the study will leverage robust cross-validation techniques such as k-fold cross-validation to evaluate the models' performance across distinct subsets of the dataset. The cross-validation technique will present insights into the stability of the models and their ability to generalize effectively to unseen data (new malware variants). Concurrently, the experiment will employ bootstrapping methods to identify potential outliers and the models' performance in varied situations. Specifically, the study will use the bootstrap resampling approach, randomly drawing samples with replacements from the original dataset to create multiple bootstrapped datasets. This will ensure that the variability in model performance is appropriately checked. The primary justification for employing two different validation methods is to gain a nuanced comprehension of the expected results.

3.6 RISK MANAGEMENT

Considering the dynamic landscape of machine learning research for malware detection, this study will implement several risk management strategies to address potential uncertainties. The areas of experiment within which these measures will be implemented include computational risks, model overfitting, and dataset limitations. The computational risks associated with the model training will be addressed through code optimization efforts and the utilization of the processing power of the GPUs, ensuring model scalability. Recognizing possibilities for overfitting, the study will use regularization methods like dropout layers for the deep learning models to ensure decent handling of unseen data. Aside from these, the earlier mention of an absence of standardized datasets for malware detection prompts this study to mitigate the challenge by employing datasets from diverse reputable sources. This will ensure that the experiment gets a good representation of all types of malware.

3.7 SUMMARY OF PROPOSAL AND PLANNED ADDITIONAL WORK TO COMPLETE

This research aims to investigate the efficacy of machine learning models in detecting new malware variants in computer systems. The study focused on employing deep learning methods like CNN and RNN and ensemble techniques to detect malware. The study's initial hypothesis was that machine-learning-driven approaches will positively affect the accuracy of detecting new malware variants. The review of existing literature, coupled with the experiment's current setup, helps to draw a guided preliminary result that confirms the hypothesis. However, an interesting realization in the study is that traditional machine learning models like the Random Forest and the k-nearest neighbour are relevant for malware detection when combined with other highly effective deep learning models. The preliminary results suggest that ensemble methods provide a high

performance in malware detection, specifically for newer malware variants. The study also finds that machine-learning approaches to detecting malware are far better than heuristic and signature-based approaches, making the findings consistent with existing research.

References

Al-Hawawreh, M., Moustafa, N., & Sitnikova, E. (2018b). Identification of malicious activities in industrial internet of things based on deep learning models. *Journal of Information Security and Applications*, *41*, 1–11. https://doi.org/10.1016/j.jisa.2018.05.002

Aslan, Ö., & Samet, R. (2020). A comprehensive review on malware detection approaches. *IEEE Access*, *8*, 6249–6271. https://doi.org/10.1109/access.2019.2963724

Eling, M., Elvedi, M., & Falco, G. (2022). The economic impact of extreme cyber risk scenarios. *The North American Actuarial Journal*, *27*(3), 429–443. https://doi.org/10.1080/10920277.2022.2034507

Firdausi, I., Erwin, A., & Nugroho, A. S. (2010, December). Analysis of machine learning techniques used in behavior-based malware detection. In 2010 second international conference on advances in computing, control, and telecommunication technologies (pp. 201-203). IEEE.

Gaurav, A., Gupta, B. B., & Panigrahi, P. K. (2022b). A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system. *Enterprise Information Systems*, *17*(3). https://doi.org/10.1080/17517575.2021.2023764

Gibert, D., Mateu, C., & Planes, J. (2020c). The rise of machine learning for detection and classification of malware: Research developments, trends and challenges. *Journal of Network and Computer Applications*, *153*, 102526. https://doi.org/10.1016/j.jnca.2019.102526

Hardy, W., Chen, L., Hou, S., Ye, Y., & Li, X. (2016). DL4MD: A deep learning framework for intelligent malware detection. In Proceedings of the International Conference on Data

Science (ICDATA) (p. 61). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

J. C. Kimmell, M. Abdelsalam and M. Gupta, "Analyzing Machine Learning Approaches for Online Malware Detection in Cloud," 2021 IEEE International Conference on Smart Computing (SMARTCOMP), Irvine, CA, USA, 2021, pp. 189-196, doi: 10.1109/SMARTCOMP52413.2021.00046.

J. Sahs and L. Khan, "A Machine Learning Approach to Android Malware Detection," 2012 European Intelligence and Security Informatics Conference, Odense, Denmark, 2012, pp. 141-147, doi: 10.1109/EISIC.2012.34.

Kamiri, J., & Mariga, G. (2021). Research Methods in Machine Learning: A content analysis. *International Journal of Computer and Information Technology*, *10*(2). https://doi.org/10.24203/ijcit.v10i2.79

LeCun, Y., Bengio, Y., & Hinton, G. E. (2015). Deep learning. *Nature*, *521*(7553), 436–444. https://doi.org/10.1038/nature14539

Lévesque, F. L., Chiasson, S., Somayaji, A., & Fernandez, J. M. (2018). Technological and human factors of malware attacks. *ACM Transactions on Privacy and Security*, *21*(4), 1–30. https://doi.org/10.1145/3210311

Madiba, T. (2022, August 29). *The role of human error in cybersecurity breach*. Engineering News. https://www.engineeringnews.co.za/article/the-role-of-human-error-in-cybersecurity-breach-2022-08-29

Naqa, I. E., & Murphy, M. J. (2015). What is machine learning? In *Springer eBooks* (pp. 3–11). https://doi.org/10.1007/978-3-319-18305-3_1

Ngo, F. T., Agarwal, A., Govindu, R., & MacDonald, C. (2020). Malicious software threats. In *Springer eBooks* (pp. 793–813). https://doi.org/10.1007/978-3-319-78440-3_35

North, D. (1968, September 1). *A tutorial Introduction to decision theory*. IEEE Journals & Magazine | IEEE Xplore. Retrieved November 13, 2023, from https://ieeexplore.ieee.org/abstract/document/4082149

Qamar, A., Karim, A., & Chang, V. (2019c). Mobile malware attacks: Review, taxonomy & future directions. *Future Generation Computer Systems*, *97*, 887–909. https://doi.org/10.1016/j.future.2019.03.007

Saad, S., Briguglio, W., & Elmiligi, H. (2019b). The Curious Case of Machine Learning In Malware Detection. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.1905.07573

Sewak, M., Sahay, S. K., & Rathore, H. (2018). Comparison of Deep Learning and the Classical Machine Learning Algorithm for the Malware Detection. *IEEE Computer Society*. https://doi.org/10.1109/snpd.2018.8441123

Sharma, A., & Sahay, S. K. (2016). An Effective Approach for Classification of Advanced Malware with High Accuracy. *International Journal of Security and Its Applications*, *10*(4), 249–266. https://doi.org/10.14257/ijsia.2016.10.4.24

Tayyab, U., Khan, F. B., Durad, M. H., Khan, A., & Lee, Y. S. (2022). A survey of the recent trends in deep learning based malware detection. Journal of Cybersecurity and Privacy, 2(4), 800–829. https://doi.org/10.3390/jcp2040041

Zhang, Y., Yang, Y., & Wang, X. (2018, March). A novel android malware detection approach based on convolutional neural network. In Proceedings of the 2nd international conference on cryptography, security and privacy (pp. 144-149)