**Summary**

There has been an increase in Cyber-attacks due to the increased use of the internet. An example is the manipulation of URLs also called malicious URLs. It has led to the stealing of personal data and economic loss. Several methods have been used to ensure secure internet surfing such as the blacklisting feature extraction and machine learning techniques. The problem with using these techniques independently from each other is that they may fail to detect newly created or changing URLs. The proposed method in this research is to develop an algorithm based on combining feature engineering with Deep Learning (DL) techniques to detect malicious URLs. This method reduces the number of false positives and improves its accuracy, thereby boosting the algorithms overall performance.

**General Limitations and Strengths**

The research question is well formulated, realistic and can be executed within a given timeframe. The proposed research is not genuinely novel; however, it is still relevant as it is currently used by various cybersecurity companies to develop antivirus software.

**Strengths and Limitations**

The proposed methodology is Experimental research which supports the research question. The process of data collection and the means of validating the performance of the model is given. One of the strengths of this methodology is that results can easily be replicated and improved upon. Also, it allows for easy manipulation of the independent variables to produce a more accurate result.

**Overall Quality**

The use of the English language is very good. The method stated were the data will be gotten from and the programming language to be used, however, it did not properly describe the dataset, that is, its size and how it would be divided for training, testing and validation. For improvement, the entire process of feature engineering and the architecture of the Deep Neural Network should be explained to make this project replicable.

For the Reference section, it is a good practice to only include papers in the reference list which were used in writing the report. That is papers such as "Liang, H., sun, X., Sun, Y. & Gao, Y., 2017. Text feature extraction based on deep learning: a review. *EURASIP Journal on Wireless Communications and Networking." AND "*Naveen, I. N. V. D., Manamohana K & Verma, R., 2019. Detection of Malicious URLs using Machine. *International Journal of Innovative Technology and Exploring Engineering,* 8(4S2 March 2019), pp. 389 -393." was not cited in the report.

In the Abstract section, the phrase "research focuses on" is used in lines 6 and 11. That is, the purpose of the research is introduced twice. Both sentences could be combined into one. For example, *'This research focuses on developing a robust and scalable algorithm by combining feature engineering and Deep Learning techniques for detecting malicious URLs'.*

In the Introduction, it is better to use an in-text citation to reference a paper rather than using the title of the paper. Lines 9-11 could be rewritten this way, *Vazhayil et al (2018) suggest using Machine Learning or Deep Learning techniques to overcome the limitations of the conventional blacklisting techniques.*

Also, the in-text citation should always be placed before the full stop rather than after. For example, this sentence in lines 11 – 13 could be rewritten this way *Moreover, the author describes the potential demerits of the machine learning algorithm and suggests the use of a Deep Learning technique for better URL detection (Vazhayil, et al., 2018).*