**Individual Report**

**Member name:** [Anuranjan Dubey](mailto:adubey37@asu.edu)

**Evaluated by:**[Krupaben Kothadia](mailto:kkothadi@asu.edu)[Sangeeth Santhosh](mailto:ssantho9@asu.edu)

**Date:** 09/02/23

**Tasks Assigned:**

* Searched 2 additional specific research papers on different Machine Learning models applied for Twitter Data.
* Craft 2 additional in-depth questions covering any specific topic in the project.
* Literature review for Machine learning techniques applied in: “Cyberthreat Detection from Twitter using Deep Neural Networks”

**Summary:**

* Question: What specific machine learning algorithms have been previously employed to enhance the accuracy and efficiency of the proposed tools in the previous research in classifying and categorizing security-related content from Twitter?
* Model excels with deep neural networks (CNN, BiLSTM), surpassing other methods, boasting a 94% true positive rate in classification and a 92% F1-score in named entity recognition.
* The method leverages deep neural networks for rapid, precise threat intel, streamlining data analysis of cybersecurity information from Twitter.
* It deploys a CNN-based binary classifier to identify security-related tweets, differentiating valuable from irrelevant ones.
* A BiLSTM NER model extracts named entities (e.g., indicators of compromise) from tweets.
* The method automates data analysis, relieving security analysts from manual data sifting.
* Deep neural networks synthesize relevant info, aiding Security Operations Centers in IT infrastructure monitoring.
* Overall, it enhances threat intel efficiency by eliminating the need for manual filtering of irrelevant data.

**Outcome:**

Simulation: The method’s effectiveness is demonstrated through simulated scenarios, it excels in classifying relevant tweets and extracting named entities.

Implementation with Experimental Data: In real-world, the method consistently performs well, achieving high accuracy in tweet classification and named entity recognition. This empirical evidence showcases its practical value for security analysts.

**References** *(with citation)*

[21] N. Dionísio, F. Alves, P. M. Ferreira and A. Bessani, "Cyberthreat Detection from Twitter using Deep Neural Networks," *2019 International Joint Conference on Neural Networks (IJCNN)*, Budapest, Hungary, 2019, pp. 1-8, doi: 10.1109/IJCNN.2019.8852475.

**Evaluation of Report  
  
Evaluation by:** [Sangeeth Santhosh](mailto:ssantho9@asu.edu) **Date:** 09/02/23

**Is the weekly member report complete with all the major result(s) of the paper(s)? If not, provide as many examples of the major result(s) missing in the written report as possible. (in bullet form). [within 100 words]**

* The individual progress report is complete with all major points covered in detail.
* The major question at hand has been answered to the point.

**Is each section of the guidelines sufficiently completed? If not, point out what is missing. [Normally within 40 words].**

Yes, each section of the guidelines has been completed to a sufficient level.

**Is the quality of this version of the written report satisfactory? If not, then why not? [Normally within 40 words]**

The quality of this version of the written report is satisfactory as it covers the tasks assigned, summary and outcome well.

**Approved by:** [Krupaben Kothadia](mailto:kkothadi@asu.edu) **Date:** 09/03/2023