**Individual In-depth Report**

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

**Evaluated by:** [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?
* Better Classification and Recognition: The tool's deep neural networks, like CNN and BiLSTM, outperform other well-known approaches. With an average true positive rate of 94% for classification and an average F1-score of 92% for named entity recognition, the tool's evaluation demonstrates outstanding accuracy rates.
* The suggested method uses deep neural networks to enable security professionals to gather fast and accurate threat intelligence without having to comb through a tonne of useless data.
* The tool consists of a processing pipeline that analyzes cybersecurity information received from Twitter.
* It uses a binary classifier, based on a Convolutional Neural Network (CNN), to identify tweets containing security-related information relevant to assets in an IT infrastructure.
* This classifier distinguishes between relevant tweets (containing valuable information) and irrelevant ones.
* Additionally, a Named Entity Recognition (NER) model, implemented as a Bidirectional Long Short-Term Memory (BiLSTM) neural network, after the embedding layer it extracts from the word level BiLSTM and tweet level BiLSTM named entities (such as indicators of compromise) from the relevant tweets.
* By automating the process of analyzing and summarizing cybersecurity information from Twitter, the tool eliminates the need for security analysts to manually sift through large amounts of data
* The deep neural networks in the tool enable it to identify relevant information and extract valuable entities, providing security analysts with synthesized knowledge. This knowledge can be used by Security Operations Centers (SOCs) to accurately monitor and secure an IT infrastructure.
* Overall, the proposed tool improves the efficiency and effectiveness of obtaining threat intelligence by reducing the manual effort required to filter through irrelevant information.

**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 summary with justification.**

The report effectively covers the machine learning techniques which are applied for detection of cyberthreats from Twitter, that are given in the research paper. The report goes in-depth to cover all major points from the research paper.

**The quality of the major result(s) with justification.**  
The results from the research paper show the effectiveness of the machine learning methods proposed using simulated and real-world data, while at the same time reducing manual effort.

**The usefulness of the paper to the overall project.**   
The paper proposes machine learning methods which will be added to the project to filter out suspicious content on social media.

**Other comments**

**Evaluation Approval  
  
Evaluation by:** [Sangeeth Santhosh](mailto:ssantho9@asu.edu) **Date:** 09/03/23

**Is the written report of the in-depth study 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). [Normally within 100 words]**

Yes, the in-depth study is complete with all major results of the paper.

**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 is 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]**

Yes, the quality of the written report is satisfactory.

**Approval.  
  
Approved by:** [Krupaben Kothadia](mailto:kkothadi@asu.edu) **Date: 09/03/2023  
  
Is the quality of this written in-depth study report and Evaluation report satisfactory? If not, then why not? (limit: 40 words)**

Yes, the quality of this written in-depth study report and evaluation report is satisfactory.