**Individual In-depth Report**

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

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

**Date:** 09/08/23

**Tasks Assigned:**

* Literature review for Machine learning techniques applied in: “CyberTwitter: Using Twitter to generate alerts for Cybersecurity Threats and Vulnerabilities”
* Write In-depth Report while comparing it to methods seen before.
* Review and Evaluate 1 other person's report.

**Summary:**

* The tool employs the SVCE(Security Vulnerability Concept Extractor) to analyze the collected data. It identifies and extracts conceptual entities linked to cybersecurity vulnerabilities from the Twitter data. This extraction process helps filter out irrelevant information and focus on key security-related content.
* Analysts create system profiles with software and hardware information. The system profile is automatically generated by the system using a tool called Facter, which is a cross-platform Ruby library for retrieving system information.
* SWRL (Semantic Web Rule Language) [3]:
  + SWRL is a language for expressing rules and logic in the context of the Semantic Web.
  + SWRL can be used to define rules that add semantic meaning to unstructured text. It converts text into structured RDF data, facilitating knowledge graph construction.
* RDF Triples (Resource Description Framework):
  + RDF is a data model for representing and structuring information on the web using triples.
  + RDF triples extract structured information from text, particularly named entities, and link them to URIs. This preprocessing enhances text data for integration into knowledge graphs and linked data.
* Named Entity Recognition (NER):
  + NER is an NLP technique for identifying and classifying named entities (e.g., people, organizations) in text. [4]
  + NER is a vital preprocessing step that extracts and classifies named entities within unstructured text. This information is used to annotate text with structured data, making it suitable for knowledge graph construction and other semantic web applications.
  + This step was also used in the “Cyberthreat Detection from Twitter using Deep Neural Networks” for separating tweets after the embedding layer it extracts from the word level BiLSTM and tweet level BiLSTM named entities.
* CyberTwitter generates personalized alerts using a knowledge base that is updated in real-time based on a user's system profile
* The intelligence extracted from Twitter is represented in RDF triples in a semantic knowledge base. Using an intelligence ontology and SWRL rules, the tool performs reasoning using the system profile, knowledge base data, and varying time slices to generate the most relevant and important threat alerts for human review.
* The paper concludes, including the use of semantic textual similarity systems to improve tweet selection, recognizing relevant tweets based on their content, and expanding the word embedding model trained on general text to include cybersecurity text.
* However, no standard metric was given to support the conclusions that this method surpasses the previously employed methods to detect security vulnerability.

**Outcome:**

The CyberTwitter system's performance was assessed through a ten-day experiment, with most alerts proving valuable. It effectively extracts cybersecurity insights from real-time Twitter data, demonstrating its capacity for issuing threat alerts.

**References** *(with citation)*

[1] S. Mittal, P. K. Das, V. Mulwad, A. Joshi and T. Finin, "CyberTwitter: Using Twitter to generate alerts for cybersecurity threats and vulnerabilities," *2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, San Francisco, CA, USA, 2016, pp. 860-867, doi: 10.1109/ASONAM.2016.7752338.

[2] 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.

[3] Horrocks, Ian, Peter F. Patel-Schneider, Harold Boley, Said Tabet, Benjamin Grosof, and Mike Dean. "SWRL: A semantic web rule language combining OWL and RuleML." W3C Member submission 21, no. 79 (2004): 1-31

[4] J. Li, A. Sun, J. Han and C. Li, "A Survey on Deep Learning for Named Entity Recognition," in IEEE Transactions on Knowledge and Data Engineering, vol. 34, no. 1, pp. 50-70, 1 Jan. 2022, doi: 10.1109/TKDE.2020.2981314.

**Evaluation of Report**

**Evaluation summary with justification.**

This research paper touches upon different tools used to generate a CyberTwitter system. The system is used to generate alerts whenever a cyberthreat occurs on Twitter. The paper successfully analyzes the results along with experimental justification.

**The quality of the major result(s) with justification.**  
The major result coming out from this paper is the usefulness of the CyberTwitter system to recognise cyberthreats and hence generate corresponding alerts. The accuracy of the system is justified by experimental results.

**The usefulness of the paper to the overall project.**   
The paper is a great asset to the overall project as it uses Natural Language Processing, Semantic Web Rule Language and other NLP techniques which add immense value to detection of suspicious activities on social media.

**Other comments**

**Evaluation Approval  
  
Evaluation by:** [Sangeeth Santhosh](mailto:ssantho9@asu.edu) **Date:** 09/10/23

**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 written report is satisfactory and complete with all major results of the paper covered in-depth.
* The main topic covered is the implementation of a cyberthreat detection system which generates alerts using NLP and other similar techniques.

**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 sufficiently detailed and hence completed.

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

Yes, the report covers each important aspect covered in the research paper in detail and hence is more than satisfactory.

**Approval.  
  
Approved by:** [Krupaben Kothadia](mailto:kkothadi@asu.edu) **Date:** 09/11/23 **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 the report is satisfactory and does not require any improvements.