**Individual Report**

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

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

**Date:** 10/28/23

**Tasks Assigned:**

* Literature review for machine learning techniques applied in: “A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection”
* Preparing an individual progress report.
* Preparing the weekly report.
* Preparing the first draft of the final report's motivation and background section.
* Writing the section on learnings, conclusions, and recommendations for machine learning in the final report.
* Reading not so important papers for research or reference.
* Review and Evaluate [Rahul Nayak](mailto:rrnayak@asu.edu)’s individual progress report.

**Summary:**

* Conducted literature review for machine learning techniques, preparing progress reports, drafting the final report's motivation and background, writing conclusions and recommendations, and reviewing Rahul Nayak's individual progress report.
* Overview of a survey paper on machine learning (ML) and data mining (DM) applications in cyber security intrusion detection.
* Categorization of intrusion detection into misuse-based, anomaly-based, and hybrid techniques.
* Discussion on the importance of data in ML/DM for cyber security.
* Addressing the challenges in cyber security and providing recommendations based on problem characteristics.
* Emphasis on the need for labeled data and the suggestion to create new datasets for research.
* Highlighting the importance of fast incremental learning for regular model updates in cyber security applications.
* Comprehensive overview of ML and DM methods in cyber analytics, especially in intrusion detection.
* Significance of cyber datasets used in ML/DM.
* Acknowledgment of the complexity of ML/DM algorithms in cyber analytics both misuse and anomaly detection.
* Noting the absence of a universally effective method for intrusion detection.

**Outcome:**

* Highlighting the importance of high-quality training and testing datasets, including network and kernel-level data.
* Addressing unique challenges in the cyber domain, particularly the need for frequent model retraining.
* Suggestion to research fast incremental learning methods for daily model updates in misuse and anomaly detection as a promising area for further investigation.

**References** *(with citation)*

[5]\* Anna L. Buczak, Erhan Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," in IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153 - 1176, 26 October 2015, doi: 10.1109/COMST.2015.2494502.

**Evaluation of Report  
  
Evaluation by:** [Sangeeth Santhosh](mailto:ssantho9@asu.edu) **Date:** 10/28/23

**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]**

Yes, the weekly member report is complete with all the major results of the paper covered in detail. The report covers the important machine learning algorithms that are applied in the research paper reviewed and discusses its importance in cyber security applications.

**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 complete, with the major application of the machine learning algorithms in cyber security applications discussed.

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

Yes, the quality of this version of the report is satisfactory.

**Approved by:** [Krupaben Kothadia](mailto:kkothadi@asu.edu) **Date: 10/30/2023**