**Individual Report**

**Member name:** [Gautham Vijayaraj](mailto:gvijaya6@asu.edu)

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

**Date: 10/20/2023**

**Tasks Assigned:**

* Preparing an individual progress report.
* Evaluating and approving team members’ individual progress and in-depth reports.
* Assigning Tasks along with the Group Leader
* Preparing the Gantt chart.
* Reading [The "Not-So-Important" Reference Papers](https://drive.google.com/drive/folders/1MpdS68DsMj4vHUt9yutzkOcZJDGQ6NkM?usp=share_link) from the References List.
* Drafting the [Summary\_Statement\_Not\_So\_Important\_Papers](https://docs.google.com/document/d/1QmxaOqG8rONc0v80Qa2wFGUMXmtyd_5nVvCeJUYJvuM/edit?usp=share_link)
* Added summary for paper [5] and [8] in the Summary Document created above.
* Providing summary of content for Individual progress report.
* Evaluating and approving the weekly report
* Taking meeting notes
* Organizing google drive

**Summary:**

* All the tasks have been completed successfully. These include assigning tasks, preparing the Gantt Chart, individual progress report, evaluating and approving the weekly report, approving 4 team members’ progress reports, taking meeting notes, reading “not so important” research papers, providing summary of content for individual progress report and organizing the google drive.
* Read 5 of the “not so important” research papers this week.
* This paper [8] addresses the growing concern of fake profiles on online social networks (OSN) by proposing a machine learning-based approach for their detection.
* The authors highlight the increasing threats to individual privacy and security on OSNs due to the exploitation of vulnerabilities.
* They present a method to collect and preprocess a dataset for training their model, using techniques like data cleaning and validation.
* Various machine learning algorithms, including Support Vector Machine (SVM), Deep Neural Network (DNN), and Random Forest, are employed to distinguish between trusted and fake profiles.
* The results are evaluated through metrics like accuracy, precision, recall, and F1 score, demonstrating the effectiveness of the proposed approach.
* The paper [5] explores machine learning (ML) and data mining (DM) methods for cyber security intrusion detection. It provides in-depth descriptions of various ML/DM techniques and their applications in identifying cyber intrusions.
* The paper classifies intrusion detection into three categories: misuse-based, anomaly-based, and hybrid techniques.
* It emphasizes the importance of data in ML/DM approaches and discusses the challenges associated with cyber security.
* The paper also offers recommendations on when to use specific methods based on the characteristics of the problem. It is a valuable resource for researchers and practitioners entering the field of ML and DM for cyber security.

**Outcome:**

One of the “not so important” papers provides a comprehensive review of ML and DM methods for cyber security intrusion detection, emphasizing the importance of labeled data and fast incremental learning. The other paper addresses the issue of fake profiles on online social networks, presenting a data-driven approach using multiple ML algorithms to distinguish genuine profiles, enhancing online security.

**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.  
  
[8] T.R Soumya, S.Solai Manohar, N.Bala Sundara Ganapathy, Leema Nelson, A. Mohan, M.Thurai Pandian. "Profile Similarity Recognition in Online Social Network using Machine Learning Approach" in International Conference on Inventive Research in Computing Applications (ICIRCA), 29 December 2022, Pages 805-809. ISSN 22473631 doi:10.1109/ICIRCA54612.2022.9985683

**Evaluation of Report  
  
Evaluation by:** [Krupaben Kothadia](mailto:kkothadi@asu.edu) **Date: 10/23/2023**

**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 weekly member's report, which includes task assignment, creating Gantt charts, and individual progress reports, is finished. In addition, five "not so important" scientific papers are reviewed. One study discusses the problem of fake profiles on social media sites and suggests a machine learning-based method for detecting them. It highlights the growing risks to people's security and privacy on these kinds of networks and offers a way to gather and prepare data. The report assesses the findings and shows that the suggested strategy is effective. Another study investigates data mining and machine learning for intrusion detection in cyber security, providing insightful analysis and suggestions for industry practitioners.

**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 completed.

**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 written report is satisfactory.

**Approved by:** [Krupaben Kothadia](mailto:kkothadi@asu.edu) **Date: 10/23/2023**