**Individual In-depth Report**

**Member name:** [Krupaben Kothadia](mailto:kkothadi@asu.edu)

**Evaluated by:** [Gautham Vijayaraj](mailto:gvijaya6@asu.edu)

**Date: 9/23/2023**

**Tasks Assigned:**

* This report summarizes the paper “[Mining user Message Pattern for Suspicious Behavior on Terrorism using NLP in Social Networks with Single Sign-On](https://drive.google.com/file/d/1STLuTC9mJx8LF8fihELth3KnG4n-0rLv/view?usp=drive_link)”. The paper delves into the realm of Data Preprocessing and NLP techniques applied within Social Networks, featuring Single Sign-On authentication. It seamlessly integrates both text and image data to detect suspicious activities, employing NLP for textual scrutiny and the LSB algorithm for steganographic image analysis, all while drawing data from Gmail and Twitter as primary sources.

**Summary:**

* This paper employs Natural Language Processing (NLP) within Social Networks, utilizing Single Sign-On authentication, to proactively identify and mitigate terrorism-related threats, with a focus on protecting lives and property. It combines text and image data for suspicious activity detection, using NLP for textual analysis and the LSB algorithm for steganographic image analysis, with Gmail and Twitter as data sources.
* Single sign-on is used for account access, and data retrieval employs JavaMail API and Twitter4j API. IMAP grants access to Gmail accounts for inbox and sent mail retrieval. The acquired data undergoes NLP processing, and resultant data patterns are stored for analysis.
* The NLP module utilizes Apache OpenNLP, employing techniques such as POS tagging (Maxent Tagger), chunking (ChunkerME API), WordNet-based semantic analysis, and spell checking. These techniques process the input dataset to derive meaningful data patterns.
* In essence, this research integrates NLP and LSB techniques to detect suspicious activities, leveraging Gmail and Twitter data with single sign-on. The NLP module, powered by Apache OpenNLP, employs various techniques to process input data and extract valuable data patterns.

**Outcome:**

The research's outcome entails an innovative approach to proactively detect and mitigate terrorism-related threats in Social Networks. By integrating Natural Language Processing and steganographic image analysis, this study showcases an effective strategy for preventing terrorist activities. The NLP module further enhances data analysis and pattern recognition capabilities, bolstering security efforts.

**References** *(with citation)*

[1] M. P. Selvan and R. Selvaraj, “Mining user Message Pattern for Suspicious Behavior on Terrorism using NLP in Social Networks with Single Sign-On,” *Indian Journal of Science and Technology*, Apr. 2017, doi: 10.17485/ijst/2017/v10i14/111364.

**Evaluation of Report**

**Evaluation summary with justification.**

The paper summarizes an approach to proactively detect and mitigate terrorism-related threats in Social Networks like Gmail and Twitter using NLP and steganographic image analysis. Their research shows an effective strategy for preventing terrorist activities. The NLP module further enhances data analysis and pattern recognition capabilities, enhancing security and threat mitigation.

**The quality of the major result(s) with justification.**  
  
The approach summarizes by combining text and image data for suspicious activity detection, using NLP for textual analysis and the LSB algorithm for steganographic image analysis, with Gmail and Twitter as data sources. The quality of the major results is not only efficient, but also provides a new area of research for further improvements.

**The usefulness of the paper to the overall project.**   
  
The steganographic image analysis to detect threats and suspicious activities on social media is very useful to the overall project. The integration of NLP and LSB techniques provides an effective strategy to prevent terrorist activities in social media.

**Other comments**

No comments

**Evaluation Approval  
  
Evaluation by:** [Gautham Vijayaraj](mailto:gvijaya6@asu.edu) **Date: 9/23/2023**

**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 with all major results for the paper.
* The integration of NLP and LSB techniques provided an effective strategy to mitigate threats in Social media like Gmail and Twitter.
* The research also mentioned that the steganographic image analysis can help eradicate and disengage terrorist activities.

**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 are sufficiently completed. The report summarized the approach, threat mitigation techniques, outcomes and usefulness to the overall project.

**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:** [Gautham Vijayaraj](mailto:gvijaya6@asu.edu) **Date: 9/23/2023  
  
Is the quality of this written in-depth study report and Evaluation report satisfactory? If not, then why not? (limit: 40 words)**

Yes, the in-depth report and evaluation report summarized the research paper with all the guidelines followed. Both reports are satisfactory and concise.