**Individual In-depth Report**

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

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

**Date:** 29th September 2023

**Tasks Assigned:**

* Literature review for Machine learning techniques applied in: “A Feature Based Approach to Detect Fake Profiles in Twitter”.
* Identifying previously read papers where methods employed in these papers like feature selection, extraction with machine learning approaches were similar.

**Summary:**

* The feature-based approach for spotting fake Twitter accounts utilized a set of 24 distinct features.
* In the study, three machine learning algorithms were employed and compared: Logistic Regression, Support Vector Machines (SVM), and Random Forest.
* Among these algorithms, Random Forest exhibited the highest performance based on accuracy, precision, recall, and F-score metrics.
* It's not explicitly stated whether this approach can be directly applied to social media platforms other than Twitter and Facebook. The study primarily focuses on these platforms.
* Several data mining tools were mentioned like snippets, including DeepScan, SybilBlind, Botometer, and COLOR+.
* DeepScan: DeepScan is a supervised machine learning-based model used for detecting malicious accounts in location-based social networks.
* SybilBlind: SybilBlind is a framework designed to detect sybils. Sybils are fake or malicious identities in a network.
* Botometer: Botometer is a bot detection tool used to combat bots on social media platforms. (Is this a good feature, with the current AI bots?)
* COLOR+: COLOR+ is a system designed to detect spam accounts in mobile social networks. It uses fog computing and defines a threshold suspicion degree to classify suspicious accounts from genuine accounts.
* The proposed methodology involves data preprocessing, feature selection, model training with supervised machine learning algorithms, and evaluation using a test dataset. The dataset is split into an 80:20 ratio for training and testing purposes.
* The primary objective is to offer a user-end solution for combating fake accounts and automated bots on social media platforms.
* The 24 features extracted for analysis encompass various categories: account-based (followers, friends, account age), tweet-based (retweets, hashtags, mentions, URLs), ownership-detail-based (domain name, ownership period), URL-based (URL length, sub-domains, SSL certificates), and others (presence of iframe, mouse hover).
* These features enhance the detection model's ability to distinguish fake accounts by analyzing account characteristics, tweet content, ownership details, and embedded URLs.
* The study doesn't explicitly state its applicability to social media platforms beyond those mentioned, leaving uncertainty about its generalizability.

**Outcome:**

The evaluation found Random Forest with 97.9% accuracy outperformed Logistic Regression (95.7%) and SVM (80.8%) in detecting fake social media accounts.

Future work includes studying human-operated fake accounts, adding features for better bot detection, incorporating tweet sentiment analysis, and developing a real-time web browser-based tool to identify bot accounts.

**References** *(with citation)*

[1] J. Kaubiyal and A. K. Jain, “A feature based approach to detect fake profiles in twitter,” Melbourn, VIC, Australia: Association for Computing Machinery, 2019, pp. 135–139. doi: https://doi.org/10.1145/3361758.3361784. Available: https://doi.org/10.1145/3361758.3361784

**Evaluation of Report**

**Evaluation summary with justification.**

The report gives an in-depth analysis of the machine learning techniques for detecting fake profiles in Twitter. The performance results of each of the algorithms are covered and the algorithm with the best performance is found.

**The quality of the major result(s) with justification.**  
The major result, which is to find the accuracy of Logistic Regression, Support Vector Machine (SVM) and Random Forest, has been done precisely in this report.

**The usefulness of the paper to the overall project.**   
The paper contributes to the overall project as it deals with detection of fake profiles which is very much related to the main project topic - Detection Process of Suspicious Activities on Social Media.

**Other comments**

Summarized nicely.

**Evaluation Approval  
  
Evaluation by:** [Sangeeth Santhosh](mailto:ssantho9@asu.edu) **Date: 1st October 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 of the in-depth study is complete with all the major results of the paper. The report covers the methodologies for each of the machine learning algorithms and compares their accuracy levels in detail.

**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 in this report of the research paper - including technique, methodology and result.

**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 and makes sure to cover all the important points mentioned in the research paper.

**Approval.  
  
Approved by:**[Krupaben Kothadia](mailto:kkothadi@asu.edu) **Date:10/02/2023  
  
Is the quality of this written in-depth study report and Evaluation report satisfactory? If not, then why not? (limit: 40 words)**

The quality of this written in-depth study report and Evaluation report is satisfactory. The evaluation report signifies correct evaluation and the report justifies the project topic by discussing various machine learning algorithms for suspicious activities detection.