**Individual In-depth Report**

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

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

**Date:** 09/22/23

**Tasks Assigned:**

* Literature review for Machine learning techniques applied in: “An effective security alert mechanism for real-time phishing tweet detection on Twitter”.
* Swapped an Irrelevant paper [2] to the important one [1].
* Write In-depth Report while comparing it to methods seen before.
* Review and Evaluate Rahul’s Report.
* Preparing Midterm Report
* Preparing Individual Midterm Review Report

**Summary:**

* Feature extraction was a crucial aspect of the mechanism's success.
* It employed a comprehensive set of 22 features spanning various categories, bolstered by 7 additional ones identified by the WEKA tool.
* This robust feature set strengthened the mechanism's ability to differentiate between phishing and legitimate tweets.
* The WEKA machine learning tool played a pivotal role in feature selection and evaluation. By incorporating the 7 additional features suggested by WEKA, the mechanism enhanced its capacity to discriminate between phishing and legitimate tweets.
* Machine learning training used a dataset with 2973 training data containing URLs from Twitter, labeled as phishing or safe.
* Beyond simulation, the mechanism's real-world implementation showcased its efficiency in live scenarios. It promptly alerted Twitter users to potential phishing URLs, a critical capability given Twitter's rapid information dissemination.
* The choice of the Random Forest machine learning technique contributed to the mechanism's success.
* RF's robustness and ability to handle complex datasets made it well-suited for phishing detection on a dynamic platform like Twitter.
* The security alert mechanism mainly detects phishing URLs, the mechanism also considers other features related to the content of the tweet, user information, and network properties.
* Features like URL length, SSL connection, Hexadecimal, Alexa rank, Age of domain - Year, Equal, Digit in host, Host length, Path length, Registrar and Number of dots in host were used in the final evaluation.

**Outcome:**

The Random Forest-based security alert mechanism demonstrated impressive performance with a precision of 94.64% and a recall of 95.49% in phishing tweet detection through simulation.

When implemented and evaluated with real Twitter and PhishTank datasets, the mechanism achieved an impressive 97.50% accuracy in promptly alerting users to phishing URLs.

**References** *(with citation)*

[1] Seow Wooi Liew, Nor, Mohd Taufik Abdullah, Razali Yaakob, and Mohd Yunus Sharum, “An effective security alert mechanism for real-time phishing tweet detection on Twitter,” Comput. Secur., vol. 83, pp. 201–207, 2019, doi:<https://doi.org/10.1016/J.COSE.2019.02.004>.

[2] A. Geiger, D. Liu, S. Alnegheimish, A. Cuesta-Infante and K. Veeramachaneni, "TadGAN: Time Series Anomaly Detection Using Generative Adversarial Networks," 2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA, 2020, pp. 33-43, doi: 10.1109/BigData50022.2020.9378139.

**Evaluation of Report**

**Evaluation summary with justification.**

The paper focuses on creating an efficient security alert mechanism for phishing detection of Twitter. Different machine learning algorithms are used to compare the performance and the best one is chosen.

**The quality of the major result(s) with justification.**  
The paper evaluates different machine learning algorithms for phishing detection on Twitter and does so by using a reliable dataset source. The research done in this study accurately touches upon the same.

**The usefulness of the paper to the overall project.**   
Overall, the paper adds useful input to the project as it provides insights into machine learning algorithms and its accuracy for phishing detection.

**Other comments**

**Evaluation Approval  
  
Evaluation by: Sangeeth Santhosh  
Date: 09/24/23**

**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 major results of the paper are covered with great accuracy in this in-depth study. It also covers the steps involved and the summary of the paper. The accuracy, precision and recall score of the Random Forest algorithm for phishing detection in Twitter has been found successfully.

**Is each section of the guidelines sufficiently completed? If not, point out what is missing. [Normally within 40 words].**

Yes, the paper satisfies all the requirements of the guidelines mentioned.

**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:**[Krupaben Kothadia](mailto:kkothadi@asu.edu) **Date: 09/24/2023  
  
Is the quality of this written in-depth study report and Evaluation report satisfactory? If not, then why not? (limit: 40 words)**

Yes, the quality of this written in-depth study report and Evaluation report is satisfactory. The evaluation report signifies that it’s been correctly evaluated and the report itself justifies the research topic that Random Forest amplifies its efficiency for the dataset having 22 features and 7 from WEKA for robust phishing detection on Twitter.