**CSG 2341 Intelligence Systems Group 5 Progress Report**

**Title –** Phishing Detection using Machine Learning

**References:**

References for the proposed project is follows,

**Journal Papers:**

1. A predictive model for phishing detection.

A. Orunsolu, A. S. Sodiya and A. T. Akinwale. Journal of King Saud University–Computer and Information Sciences, <https://doi.org/10.1016/j.jksuci.2019.12.005>

1. Fighting against phishing attacks: state of the art and future challenges.

B. B. Gupta, Aakanksha Tewari, Ankit Kumar Jain, and Dharma P. Agrawal. 2017. Neural Comput. Appl. 28, 12 (December 2017), 3629–3654. DOI: <https://doi.org/10.1007/s00521-016-2275-y>

1. Towards detection of phishing websites on client-side using machine learning based approach.

Jain, A. K., & Gupta, B. B. (2018). Telecommunication Systems, 68(4), 687–700.

1. Machine learning based phishing detection from URLs. Expert Syst.

Sahingoz, O.K., Buber, E., Demir, Ö., & Diri, B. (2019). Appl., 117, 345-357.

**Conference Papers:**

1. Using machine learning to deal with Phishing and Spam Detection: An overview.

Lazaar, Saiida. (2020).

1. Applying Machine Learning Techniques to Detect and Analyze Web Phishing Attacks.

Cuzzocrea, Alfredo & Martinelli, Fabio & Mercaldo, Francesco. (2018). iiWAS2018: Proceedings of the 20th International Conference on Information Integration and Web-based Applications & Services. 355-359. 10.1145/3282373.3282422.

1. A machine-learning framework for supporting intelligent web-phishing detection and analysis.

Cuzzocrea, Alfredo & Martinelli, Fabio & Mercaldo, Francesco. (2019). IDEAS '19: Proceedings of the 23rd International Database Applications & Engineering Symposium. 1-3. 10.1145/3331076.3331087.

1. Efficient Detection of Phishing Attacks with Hybrid Neural Networks. X. Zhang, D. Shi, H. Zhang,

W. Liu and R. Li. 2018 IEEE 18th International Conference on Communication Technology (ICCT), Chongqing, 2018, pp. 844-848, doi: 10.1109/ICCT.2018.8600018.

1. Perception of a New Framework for Detecting Phishing Web Pages.

Mourtaji, Youness & Bouhorma, Mohammed & Alghazzawi, Daniyal. (2017). 10.1145/3175628.3175633.

1. Learning-based models to detect runtime phishing activities using URLs.

Surya Srikar Sirigineedi, Jayesh Soni, and Himanshu Upadhyay. 2020 In Proceedings of the 2020 the 4th International Conference on Compute and Data Analysis (ICCDA 2020). Association for Computing Machinery, New York, NY, USA, 102–106. DOI:https://doi.org/10.1145/3388142.3388170

1. Phishing URL Detection via CNN and Attention-Based Hierarchical RNN.

Y. Huang, Q. Yang, J. Qin and W. Wen. 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 2019, pp. 112-119, doi: 10.1109/TrustCom/BigDataSE.2019.00024.

1. Phishing Website Detection Based on Machine Learning: A Survey.

C. Singh and Meenu. 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2020, pp. 398-404, doi: 10.1109/ICACCS48705.2020.9074400.

1. PHISH-SAFE: URL Features-Based Phishing Detection System Using Machine Learning.

Jain A.K., Gupta B.B. (2018). In: Bokhari M., Agrawal N., Saini D. (eds) Cyber Security. Advances in Intelligent Systems and Computing, vol 729. Springer, Singapore.

1. Using Lexical Features for Malicious URL Detection - A Machine Learning Approach.

Joshi, A., Lloyd, L., Westin, P., & Seethapathy, S. (2019). ArXiv, abs/1910.06277.

**Group 5 Team Contract for CSG2341**

**Project Team Name:** Group 5

**Project Team Members**: YONG HAN Tan, PHONE TOE Kyaw, DAVID SELVAM Visahl Samson

**Code of Conduct:** As a project team, we will:

* Cannot be late to the meeting
* Only talk about the project during the meeting

**Participation:** We will meet and discuss project matter a minimum of 1 time per week:

* Members need to either reach to PSB Academy study area or Digital platforms such as Skype, Zoom, Microsoft Teams, and Blackboard Collaborate at 6 PM every Tuesday.
* All group members are required to be punctual in joining meetings.
* Group members must take turns listening and talking as everyone should contribute and have a say (only one person talking would be appropriate while a new feature is being demonstrated)
* Group members must take turns recording the minutes of each meeting in addition to updating any allocated tasks and their agreed upon deadlines. 10. All members must be made aware of and contribute towards any decisions before they are officially made.
* Group members are required to share files/work in the agreed upon collaboration platform (such as the group’s File area).

**Communication:** We will:

* Email, WhatsApp, Blackboard group forums.
* Team members agree to complete major correspondence to ALL other members and not to single entities.

**Conflict Resolution:**

* Conflicts that occur should be mentioned to and be discussed by the whole group to ensure everyone is on the same page.
* If a group member misses a deadline without a valid reason, that group member will be issued a formal warning and the tutor and unit coordinator will be notified.
* Member who do not come to meeting for two weeks, will be ejected from the group.

**Meeting Guidelines:** We will:

* Recorded, Notes, placed in University’s one drive.

**Project Team Members Names, Roles and Sign-off:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Student No.** | **Role** | **Sign-off on Team Contract** |
| DAVID SELVAM Visahl Samson | 10498743 | Team Leader | |  | | --- | |  | |  | |  | |
| PHONE TOE Kyaw | 10502161 | Tester |  |
| YONG HAN Tan | 10505415 | Developer |  |