SIT719 Security and Privacy Issues in Analytics

Distinction/HD Task 9.1 9.1 Technical Review Article on Security, Privacy and Analytics

Overview

At this point, you have gained a clear knowledge on how machine learning or AI can help to solve issues related to security and privacy.

In this *HD Task*, you have to review the literature, read existing surveys and technical articles, explore blogposts, news items and gather information to write a technical review article by your own. Please see more details in Task description. Before attempting this task, please make sure you are already up to date with all ***Credit and Pass tasks and task 5.1 (D)***.

Task Description

Instructions:

Choose **one topic** from the four given topics below. You can prefer any one of the topics based on your choice and preference. Write **minimum 6000 word review** (excluding tables (if any), figures (if any), equations (if any), and references) based on your selected topic. For your benefit, I have included some sections. But you are free to add/modify sections and subsections to make the review article more informative, organized and readable. If you want to achieve a D/HD grade, you have to demonstrate expert/superior learning outcomes in the area of security, privacy and analytics. Therefore, you have to write in such a way that it may target audiences who have domain knowledge and find your article interesting and insightful. Please see the judging criteria (rubric) at the end of this task sheet.

Choose any one of the below topics to submit this task.

Topic 1:

Securing Industrial infrastructure against cyber-attacks using machine learning and artificial intelligence at the age of Industry 4.0

Sections you may include (but not limited to): Introduction, background of Industry 4.0, Importance of data sharing, Cyber risk at the age of Industry 4.0, Combating cyber-attacks using advanced analytics, real-world use cases, future opportunities, conclusion

Sample Reference:

1. https://www2.deloitte.com/content/dam/insights/us/articles/3749_Industry4-0_cybersecurity/DUP_Industry4-0_cybersecurity.pdf

2. https://books.google.com.au/books?hl=en&lr=&id=1-FY-U30lUYC&oi=fnd&pg=PP1&dq=cybersecurity+machine+learning+and+AI&ots=cFNgE6Nbi7&sig=NeBYNzF9XOJtEs6ziWqHoBO9Edo#v=onepage&q=cybersecurity%20machine%20learning%20and%20AI&f=false

Topic 2:

Recent advancement of Machine Learning and AI for Cyber Security Intrusion Detection

Sections you may include (but not limited to): Introduction, Background of IDS, Major advancement in ML and AI, datasets used for IDS (a big list of datasets and their qualitative comparison), state-of-the-art techniques, use-case/example case study, future trends, and conclusion.

Sample Reference:
1. https://ieeexplore.ieee.org/document/7307098

Topic 3:

Privacy-preserving analytics for social network data: A survey on anonymization techniques

Sections you may include (but not limited to): Introduction, Privacy attacks using social network data, Challenges in anonymizing social network data, state-of-the-art techniques, commercial and open-source tools for privacy analytics (list and compare at least 5), practical use-case/example case study, future trends, and conclusion.

Sample Reference:

1. https://www.cs.sfu.ca/~jpei/publications/SocialNetworkAnonymization_survey.pdf (published in 2008, so there is a scope to explore lots of new information that I will expect you will cover)

Topic 4:

Differential Privacy for real-world applications: past, present and future

Sections you may include (but not limited to): Introduction, Background of differential privacy, why DP over anonymization and encryption, Motivation of using DP for real-word applications, commercial and open-source tools for privacy analytics (list and compare at least 15), DP for internet system, DP for Healthcare, DP for Energy System, DP for IoT, DP for transportation system, DP for smart farming, etc, future trends, and conclusion.

Sample Reference:
1. https://arxiv.org/pdf/1812.02282.pdf
2. https://privacytools.seas.harvard.edu/files/privacytools/files/pedagogical-document-dp_new.pdf

Convert the report into a PDF document and check for plagiarism from the unit site of the CloudDeakin (under “assignments” of the “assessment” tab). Ensure that the similarity score is less than 20%. Take a screenshot of the similarity score and attach at the end of the PDF and submit using OnTrack system.

Criteria	Unsatisfactory – Beginning	Developing	Accomplished	Exemplary	Total
Review Article Focus: Purpose/ Position Statement	**0-7 points**	**8-11 points**	**12-15 points**	**16-20 points**	/20
	Fails to clearly relate the review article topic or is not clearly defined and/or the article lacks focus throughout.	The review is too broad in scope (outside of the title topic) and/or the review is somewhat unclear and needs to be developed further. Focal point is not consistently maintained throughout the article.	The review article provides adequate direction with some degrees of interest for the reader. The article states the position, and maintains the focal point of the article for the most part.	The article provides direction for the paper that is engaging and thought provoking. The article clearly and concisely states the position, and is consistently the focal point throughout the paper.	
Literature review	**0-14 points**	**15-24 points**	**25-39 points**	**40-50 points**	/50
	Demonstrates a lack of understanding and inadequate literature of the topic. Review is superficial based on opinions and preferences rather than critical selection of existing literature. Review at least 10 references.	Demonstrates general understanding with limited critical literature related to the topic. Review at least 15 references.	Demonstrates good level of understanding with adequate literature review related to the topic. Good demonstration but could be further improved based on critical analyses of the exiting literatures by providing expert opinion or comments with supportive logic and evidence. Review at least 20 references.	Demonstrates superior level of understanding with adequate literature review related to the topic. Compares/contrasts perspectives, considers counter arguments or opposing positions, and draws original and thoughtful conclusions with future implications based on the literature survey. Review at least 30 references.	
Writing Quality & Adherence to Format Guidelines	**0-7 points**	**8-14 points**	**15-21 points**	**22-30 points**	/30
	Article shows a below average/poor writing style lacking in elements of appropriate standard English. Frequent errors in spelling, grammar, punctuation, spelling, usage, and/or formatting.	Article shows an average and/or casual writing style using standard English. Some errors in spelling, grammar, punctuation, usage, and/or formatting.	Article shows above average writing style (can be considered good) and clarity in writing using standard English. Minor errors in grammar, punctuation, spelling, usage, and/or formatting.	Article is well written and clear and standard English characterized by elements of a strong writing style. Basically, free from grammar, punctuation, spelling, usage, or formatting errors.	

Rubric idea adopted from: Denise Kreiger, Instructional Design and Technology Services, SC&I, Rutgers University, 4/2014