**Individual In-depth Report**

**Member name:** [Gautham Vijayaraj](mailto:gvijaya6@asu.edu)

**Evaluated by:** [Krupaben Kothadia](mailto:kkothadi@asu.edu)

**Date: 10/09/2023**

**Tasks Assigned:**

* Focus on my question to work upon as my area of research for this project.
* The question I chose was to do my research and find a system that maintains the balance between detecting suspicious activity in social media and safeguarding the user's privacy and maintaining data integrity.
* Review of [**Privacy Preservation of Social Network Users Against Attribute Inference Attacks via Malicious Data Mining**](https://drive.google.com/file/d/1Gigpwllq6nNhbfu33l_-eNO7mxQF0CTZ/view?usp=drive_link)

**Summary:**

* The main focus area of this paper is to address the growing concern of privacy in online social networks (OSNs) where users often share personal information.
* The authors introduce a privacy-preserving technique called 3LP+, which is an extension of the existing 3LP algorithm.
* While 3LP was designed to protect a single sensitive attribute, 3LP+ aims to safeguard multiple sensitive attributes that users may have, such as political views and sexual orientation.
* The key innovation in 3LP+ is its coordinated approach to preserving privacy across multiple attributes, avoiding conflicts that may arise when multiple runs of the algorithm are used independently.
* The privacy attack scenario discussed in the paper involves a malicious data mining approach. Attackers gather user data, including regular attributes (e.g., relationship status and profession) and link attributes (derived from friendship connections). They use this data to build decision trees and predict sensitive attributes, even if the user has not explicitly shared them.
* The 3LP+ technique is presented in three layers :
  + **Attribute Suppression (Layer 1):** In this layer, 3LP+ computes the sensitivity of each attribute and suggests to the user which attribute values to suppress. It generates sensitive rules and identifies the attributes that, when suppressed, would provide the most privacy protection. The decision to suppress an attribute ultimately rests with the user.
  + **Hiding Friendship Links (Layer 2):** If sensitive rules in Layer 1 still pose a threat (particularly those relying on link attributes), 3LP+ recommends hiding friendship links to disrupt the attacker's predictions. It selects links to hide strategically to minimize the impact on the user's social connections.
  + **Adding Friendship Links (Layer 3):** If sensitive rules involve link attributes that need to exceed a certain threshold, 3LP+ suggests adding new friends to the user's network. This helps make the rule inapplicable and further protects the user's privacy.

**Outcome:**

* The reference paper explores a privacy-preserving technique, 3LP+, designed to protect users in online social networks from attribute inference attacks.
* The experimental results suggest that it outperforms existing techniques, even when attackers use different classifiers. 3LP+ offers better privacy protection for users with multiple sensitive attributes compared to existing techniques.

**References** *(with citation)*  
  
[42] Khondker Jahid Reza, Md Zahidul Islam and Vladimir Estivill-Castro,”Privacy Preservation of Social Network Users Against Attribute Inference Attacks via Malicious Data Mining”, in Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP 2019), Barcelona, Spain, pp. 412-420, doi: 10.5220/0007390404120420

**Evaluation of Report**

**Evaluation summary with justification.**

This report discusses the 3LP+ privacy-preserving technique for safeguarding multiple sensitive attributes in online social networks (OSNs). It addresses privacy concerns arising from malicious data mining attacks and presents a three-layered approach. The innovation in 3LP+ lies in its coordinated protection of attributes, reducing conflicts. This report offers a comprehensive solution to enhance user privacy in OSNs.

**The quality of the major result(s) with justification.**  
The quality of the major result, 3LP+ privacy-preserving technique, is justified by its innovative approach to safeguarding multiple sensitive attributes effectively.

**The usefulness of the paper to the overall project.**   
The paper enhances the project by introducing 3LP+ as a multi-attribute privacy-preserving technique, safeguarding user data in online social networks.

**Other comments**

Report is very well written.

**Evaluation Approval  
  
Evaluation by:** [Krupaben Kothadia](mailto:kkothadi@asu.edu) **Date: 10/09/2023**

**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 report on the in-depth study is comprehensive, encompassing all major findings. The paper introduces 3LP+, a privacy-preserving method for online social networks (OSNs). Unlike its predecessor, 3LP, it safeguards multiple sensitive attributes, addressing privacy concerns such as political views and sexual orientation. 3LP+'s innovation lies in its coordinated approach across these attributes, minimizing conflicts. The paper also discusses a privacy attack scenario involving malicious data mining. It elaborates on 3LP+'s three-layer technique, covering attribute suppression, hiding friendship links, and adding new connections to protect user privacy effectively. Thus, the report provides a complete overview of the paper's significant results.

**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 completed. The paper addresses privacy concerns in online social networks, introduces 3LP+ as an innovative privacy-preserving technique, and elaborates on its three-layer approach to safeguarding sensitive attributes effectively.

**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.

**Approval.  
  
Approved by:** [Krupaben Kothadia](mailto:kkothadi@asu.edu) **Date: 10/09/2023  
  
Is the quality of this written in-depth study report and Evaluation report satisfactory? If not, then why not? (limit: 40 words)**

Yes, the report is evaluated by me and the report has been studied carefully with all the remarks added in the evaluation report. The quality of this written in-depth study report and evaluation report is satisfactory.