# Review of Prüfungsleistung

Gutachter*in: Amelie Sophie Robrecht

10.04.2025

| | |
|---|---|
| Author | Syed Zain Ali |
| Topic | *Privacy and Security in Federated Learning* |
| Course | AI Know You so Well - Personalization and User Modeling in Intelligent Systems |

**Content and Research Question** The student compares current approaches on FL focusing on privacy and security. The main research question is: Which problems is FL currently facing and how are those challenges handled in the context of user profiling and personalization?

**Abstract and Introduction** **5/5 good** The **abstract** fulfills the requirements. It is comprehensive and easy to follow. The topic, its relevance and the papers used for the comparison are discussed. The publication type of the compared papers does become clear.

The list of keywords is missing.

The introduction is well done. Motivation and relevance of the topic is introduced and supported by literature. The term personalization is introduced and diverging definitions are discussed. Challenges federated learning is facing (fairness vs. accuracy) are stressed. The objectives become clear.

The student gives a good and well-founded definition of the term federated learning. The structure of the paper is described.

**Methods** **4/5 good** This second approach includes a methodology section. The selection of literature is described, keywords and platforms used are listed. The papers compared are experimental and research papers. The objective of the comparison is made clear. It would be helpful to list all the papers used as main content for the comparison so the reader can distinguish between those main papers and background papers.

**Comparison/Main** **5/5 very good** In the **Overview& Background** section, the motivation becomes very clear. The student clusters the papers very well by their FL architectures. Also a more detailed definition of the term FL is given and arguments for FL are given, supported by literature. Again the student relates data security and FL back to personalization. The section **challenges in FL** talks about the challenges discussed in the papers. The student again shows how those challenges are especially problematic when it comes to fairness in personalized models. The sections **User Modeling and Federated Learning** and **Personalization and Federated Learning** allow a better understanding of how FL is connected to the seminar's topic. Adding those chapters makes the paper a more coherent and better to follow submission. In the section **privacy in federated learning** the student describes how fairness can be integrated into federated learning. Different approaches, such as differential privacy, LDP, or SMC are introduced. In the section **security in FL** the student gives a very good distinction of the terms security and privacy, to then talk about different potential vulnerability aspects of FL and some defense approaches. Some of the approaches are just listed, but not at all introduced or discussed and they never come up again.

Overall, the student gives a good overview of privacy and security issues and sets it into the context of the seminar's objective. The differentiation of individual aspects (e.g. privacy and security) is particularly convincing.

**Discussion 4/5 good**

The student discusses the outcomes of the papers, but also the gaps that remain open. In addition, the student relates back to potential problems introduced in the introduction, which is very good. Findings from the main part are discussed and compared, future perspectives are developed from this. While the main part could be a little shorter, the discussion should be more detailed.

**Conclusion 5/5 very good** The conclusion is well done. The added value of one's own work is realistically summarized and several potential future work directions are named. I would also like to positively emphasize the list of abbreviations that the student has attached to the paper.

**Paper Selection 3/5 adequate** It is hard to figure out which of the papers are used for the main comparison and which are background papers. Apart from this the student used a remarkably large amount of papers. The papers selected for the comparison do match the research question. The papers used for the main comparison are all of high quality. Some of the papers used for background information are arxiv papers, which is perfectly fine. The student has used a lot of additional literature. The literature works well with the topic of the paper.

**Style 3/5 adequate** The literature references are not entirely consistent. Sometimes places, dois and URLs are included, sometimes not. The citation style used is coherent, but the student does not use in-text citations correctly (citet). The student does not use the requested template (but a related one), so some of the style requirements are not fulfilled (keywords are missing). The student did not use AI support for his writing. The text is written coherent and mainly correct. Some minor formulation issues are highlighted in the PDF. Especially in the main section the student overuses bullet points. The paper is way too long, while 5-6 pages were requested the main part of the paper is 10 pages.

**Review 3/5 adequate** The student gives a well funded description of state of the art FL approaches and how those are related to personalization and user modeling.

This paper is a second approach, which is influencing the final grading. The student did include the criticized aspects very well.

I thus grade this paper

**—2,3 —**

Bielefeld, 10.04.2025

Amelie Sophie Robrecht