ABSTRACT

of the PhD thesis by Bakirova Gulnaz Sailauovna on « Development of models and methods using federated machine learning», submitted for the degree of Doctor of Philosophy (PhD) in the EP 8D06102 – Computer and Software Engineering

Relevance of the research. The educational environment is entering an era of global digitalization, which is why there is steady development of tools for analyzing distributed and confidential data in this field. In connection with this, there is active growth in scientific and practical interest in federated machine learning methods. Stricter requirements for the protection of confidential data when collecting large amounts of information limit the possibilities of centralized processing. Preserving the confidentiality of data reflecting the learning activity, behavioral characteristics, and psycho-emotional state of students collected in modern educational systems is a particularly important task.

The potential of federated learning when working with distributed data is confirmed by the results of foreign studies. The accuracy of models, which is comparable to centralized learning, is ensured by the basic mechanism of federated aggregation. Unstable convergence and a decrease in the quality of the global model are characterized in conditions of unbalanced and heterogeneous data, which is reflected in the studies. Improved federated learning schemes have been proposed in the scientific literature to overcome these limitations. Approaches based on server optimization are aimed at increasing the stability and accelerating the convergence of the learning process, and methods using proximal regularization allow limiting the divergence of local models and stabilizing learning in conditions of data heterogeneity. The possibility of achieving high accuracy without transferring source data between clients is reflected in additional research in the field of horizontal federated learning.

Issues related to personal data protection receive special attention in scientific literature. Federated learning is one of the most promising methods for educational and social systems, allowing for a combination of analytical efficiency and compliance with information security requirements.

An analysis of research has shown that in the field of federated learning, most work is primarily focused on differentiable models and neural network architectures. The application of federated approaches to non-differentiable machine learning algorithms, in particular to ensemble models such as Random Forest. The development of federated aggregation methods based on statistical representations of local models remains insufficiently studied. Practical implementation for analyzing the psycho-emotional state of students based on real heterogeneous data from educational institutions has a limited number of mentions in the scientific literature.

The task of developing and implementing federated machine learning methods for non-differentiable models for analyzing distributed confidential student

data is relevant. The solution to this task is to ensure a high level of personal information protection, improve the stability and quality of global models in heterogeneous data environments, develop the digital transformation of the educational environment, and introduce intelligent analytical systems in strict compliance with information security requirements.

The goal of this dissertation research is to develop models and methods for federated machine learning and their practical implementation for analyzing distributed confidential data while ensuring personal information protection requirements and learning stability in heterogeneous data environments.

Research objectives:

1. Implement a system for collecting, preprocessing, and reconciling the feature space of distributed student data.
2. Develop federated aggregation methods for non-differentiable ensemble models based on statistical representations of local models.
3. Develop a federated machine learning architecture for analyzing distributed confidential data with local information processing without transferring the source data to the server.
4. Conduct an experimental evaluation of the effectiveness, stability, and convergence of the developed models in heterogeneous non-IID data conditions.

The object of the research is the educational environment in which distributed confidential student data is generated and used to analyze and predict their psycho-emotional state using federated machine learning methods.

The subject of the research is methods and algorithms of federated machine learning designed to analyze and predict the psycho-emotional state of students based on distributed and heterogeneous data while ensuring information confidentiality.

Research methods:

1. System analysis and design methods for developing the architecture of a federated learning system and web platform.
2. Methods for preliminary data processing and transformation: cleaning, validation, anomaly handling, feature encoding, and time series transformation.
3. Ensemble and federated machine learning methods based on the aggregation of statistical representations of local models.
4. Methods of mathematical statistics and computational experiments for assessing the quality, stability, and convergence of the global model.

The scientific novelty of the research lies in the following:

1. An approach to modifying and extending federated machine learning for the non-differentiable ensemble model Random Forest Regression has been developed and implemented based on replacing the classical aggregation of model parameters with the aggregation of statistical representations of local models, namely, feature importance vectors, which ensures the stability of the learning process in conditions of heterogeneous (non-IID) data distributions.
2. Models and methods of federated machine learning have been developed for the analysis of distributed confidential data, ensuring local information

processing, global model stability, and data confidentiality when working in real-world distributed educational environments.

3. A federated learning architecture has been proposed that ensures the formation of a global model based on local updates without transferring client source data to the server, which allows compliance with confidentiality and personal information protection requirements.

Theoretical significance of the research: studying issues of distributed data analysis based on machine learning theory. We applied FedAvg, FedOpt, and FedProx as federated learning algorithms on decentralized datasets and Random Forest Regression as an ensemble machine learning model for predictions, as well as classical statistical analysis methods and data preprocessing as key methods used in the study. The work followed standard machine learning steps from data preparation to result evaluation. It was implemented in Python using the sckit-learn, pandas, NumPy, and matpotlib libraries, which simplified the experiments and made the visualization clear.

Practical significance of the research: The research is aimed at developing and expanding federated machine learning methods by developing and implementing an approach adapted for the non-differentiable ensemble model Random Forest Regression. The work proposes replacing the classical aggregation of model parameters with the aggregation of statistical representations of local models in the form of feature importance vectors, which ensures the stability of the learning process in conditions of heterogeneous (non-IID) distributed data.

A federated learning architecture has been developed that allows the formation of a global model based on local updates without transferring client source data to the server, which ensures compliance with confidentiality and personal information protection requirements.

Main provisions put forward for defense:

• Federated machine learning architecture has been developed and implemented for analyzing distributed and confidential student data, enabling local models to be trained without transferring source information to the server and complying with personal data protection requirements.

• The FedAvg, FedOpt, and FedProx federated learning algorithms were adapted to the non-differentiable Random Forest Regression model by replacing weight aggregation with the aggregation of statistical representations—feature importance vectors, which ensured learning stability with heterogeneous (non-IID) data.

• Comparative analysis of the effectiveness of federated aggregation algorithms on real distributed data reflecting the psycho-emotional state of students was conducted, showing that FedProx provides the greatest stability for non-IID distributions, while FedOpt accelerates the convergence of the global model.

The dissertation research yielded the following scientific results, which determine its scientific novelty:

• System for collecting, preprocessing, and coordinating the feature space of distributed student data has been implemented.

• Methods of federated aggregation for non-differentiable ensemble models based on statistical representations of local models have been developed.

• Architecture for federated machine learning has been developed for analyzing distributed confidential data with local information processing without transferring the source data to the server.

• An experimental evaluation of the effectiveness, stability, and convergence of the developed models in heterogeneous (non-IID) data conditions has been conducted.

The main results of the work were presented and discussed at seminars held by the Department of Computer Engineering at the IITU (2022–2026) and in Tenaga Nasional university in Malaysia (2024–2026). A total of 8 publications were produced on the dissertation topic: 1 article in journals indexed in international databases such as Web of Science и Scopus, 4 articles in journals recommended by the Committee for Quality Assurance in Science and Higher Education of the Ministry of Education and Science of the Republic of Kazakhstan; 2 articles were published in IITU, Special issue; 1 article in the Bulletin of KazNTU, Computing & Engineering.

1. Bakirova G. S., Bektemyssova G. U., Nor'ashikin Binti Ali. Federated Machine Learning for Monitoring Student Mental Health in Kazakhstan. International Journal of Advanced Computer Science and Applications. E-ISSN: 2156-5570 P-ISSN: 2158-107X. Volume 16 Issue 10. 2025. стр. 212–220. CiteScore - 2. Highest percentile –47%. Quartile - Q3. https://thesai.org/Downloads/Volume16 No10/Paper_22-Federated_Machine_Learning_for_Monitoring_Student_Mental_Health.pdf

2. Bakirova G. S., Bektemyssova G. U. Analysis of federated learning algorithms. Bulletin of KazATK, Bulletin of the Kazakh Academy of Transport and Communications named after M. Tynyshpaev, ISSN 2790-5802, - Том 131 №2, - 2024г. С.: 297-304 DOI: https://doi.org/10.52167/1609-1817-2024-131-2-297-304.

3. Bakirova G. S., Bektemyssova G. U. Comparative analysis of unified machine learning algorithms. Scientific Journal of Astana IT University. ISSN (P): 2707-9031 ISSN (E): 2707-904X, Volume 17, March 2024, P.:57-67. DOI: 10.37943/17BVCN7579.

4. Bakirova G. S., Bektemyssova G. U., Yermukhanbetova Sh., Shyntore G. A., Umutkulov D. B., Mangysheva Zh. S. Analysis of the relevance and prospects of applying federative learning. Bulletin NIA RK, №2(92), 2024, С.: 56–65 DOI: 10.47533/2024.1606-146X.262_2024-w.pdf

5. Bektemyssova G. U., Akhmer E. Zh., Sabdenov A., Bakirova G. S., Development of a model for document classification (using passports as an example). Bulletin of KazATK, Bulletin of the Kazakh Academy of Transport and Communications named after M. Tynyshpaev, ISSN 2790–5802, - Том 136 №1, - 2025г. -С. 393–401 DOI: https://doi.org/10.52167/1609-1817-2025-136-1-393-401

6. Bakirova G. S., Bektemysova G. U. Review of distributed and federated machine learning for big data models. International Journal of Information and Communication Technologies, Special Issue 2023. ISSN 2708–2032 (print) ISSN

2708–2040 (online), Спецвыпуск 2023. стр. 89-96. https://ydf.iitu.edu.kz/files/26-37-PB.pdf

7. Bakirova G.S., Bektemyssova G.U. Analysis of probable threats in the use of federated learning and their protection methods . International Journal of Information and Communication Technologies, Special Issue 2024. ISSN 2708–2032 (print) ISSN 2708–2040 (online), стр. 64-69. ttps://ydf.iitu.edu.kz/files/%D0%A1%D0%BF%D0%B5%D1%86%D0%B2%D1%8B%D0%BF%D1%83%D1%81%D0%BAYDF2024.pdf

8. Bakirova G.S., Bektemyssova G.U., Shaikemelev G. Applications in federated machine learning. Bulletin of KazNTU, Computing & Engineering, Volume 1 №3, - 30.09. 2023г. С.: 25-28, DOI: https://doi.org/10.51301/ce.2023.i3.05

9. Bakirova G. S., Bektemyssova G. U. Certificate of the right to protect a computer program № 62530 Республики Казахстан. Analysis system for identifying signs of psycho-emotional burnout in students using federative learning methods. Application 26.09.2025; publication 30.09.2025.

Results. In the course of the research, current approaches to federated machine learning were studied, with particular attention paid to the FedAvg, FedOpt, and FedProx algorithms, taking into account issues of stability and convergence of models with heterogeneous (non-IID) distributed data. Analysis of scientific publications showed that federated learning is a promising tool for processing confidential information, but its application to non-differentiable models remains insufficiently studied.

A federated learning architecture for analyzing distributed data that reflects the psycho-emotional state of students was developed and implemented as part of the study. Let's take a closer look at the architecture, which consists of local models trained on the client side using Random Forest Regression, which provides high prediction accuracy and resistance to data noise, and global models trained on the server side, which means that the server part performs aggregation without access to the source data.

Data collection was carried out via a web platform sent to all clients over a two-month period from September 1 to October 30. The information base included data on nutrition, physical activity, sleep and rest, psycho-emotional state, as well as time and identification attributes. Data was collected from several educational institutions, which made it possible to simulate conditions of real heterogeneity. Preliminary data preparation included cleaning up incorrect records, filtering out outliers, converting time attributes to numerical format, and encoding the categorical identifier student_id using the One-Hot Encoding method. We verified the consistency of the feature space between local datasets, which is necessary for correct federated aggregation.

The FedAvg, FedOpt, and FedProx federated learning algorithms were adapted to the non-differentiable Random Forest Regression model by replacing the aggregation of model weights with the aggregation of statistical representations, i.e., feature importance vectors, which preserves the mathematical logic of federated learning and ensures the stability of the global model.

A comparative analysis of federated aggregation algorithms was performed using regression and classification metrics. The results showed that it provides a basic level of quality and will be used as a benchmark, although its convergence deteriorates with pronounced data heterogeneity. In turn, it demonstrates accelerated convergence through the use of server optimization, but provided the most stable training and minimal quality fluctuations. The dynamics of the accuracy and loss functions of global models were analyzed by rounds of federated learning. All algorithms show a steady increase in accuracy and a monotonic decrease in Centralized Loss, which demonstrates correct convergence and the absence of overfitting. Consequently, the goals and objectives of the dissertation research were achieved, and the results obtained confirm the effectiveness of applying adapted federated learning methods for analyzing the psycho-emotional state of students on distributed confidential data and are of both scientific and practical significance.

The first chapter discusses the main approaches to federated learning and justifies the choice of synchronous horizontal Cross-Silo federated learning. The use of a unified feature space allowed for the correct aggregation of local results without transferring the source data. The architecture ensured stable convergence of the global model, preservation of confidentiality, and training efficiency in heterogeneous data conditions, confirming the applicability of the proposed solution in an educational environment.

The second chapter examines federated learning algorithms and architectures, showing that the basic FedAvg and FedSGD methods ensure data confidentiality but lose stability with non-IID distributions. In turn, FedOpt and FedProx increase stability and accelerate convergence through proximal regularization and server optimization. As a result, choosing FedAvg, FedOpt, and FedProx is the most balanced solution for analyzing distributed confidential data.

The third chapter is devoted to describing a web platform for collecting data on students' nutrition, physical activity, sleep, and psycho-emotional state, as well as the use of the Maslach Burnout Inventory (MBI) questionnaire and its adaptation for research. Methods for processing non-IID data, ensuring confidentiality, and mathematical models for analyzing psycho-emotional state are considered. Algorithms for predicting burnout, principles of data coding, and automated analysis of factors affecting the level of burnout are described. The limitations of the study and prospects for further development of the proposed approach are also outlined.

The fourth chapter presents a comparative analysis of the FedAvg, FedOpt, and FedProx federated learning algorithms for predicting students' psycho-emotional burnout. It is shown that FedAvg is of limited effectiveness with non-IID data, while FedOpt provides faster and more stable convergence through server optimization, and FedProx improves training stability through proximal regularization, but with slower convergence. As a result, FedOpt is chosen as the main algorithm, FedProx as a stable solution for highly heterogeneous data, and FedAvg is used as the baseline.

The fifth chapter is devoted to describing a web platform for collecting data on students' nutrition, physical activity, sleep, and psycho-emotional burnout, as well as analyzing the structure and adaptation of the Maslach Burnout Inventory

(MBI) questionnaire. Methods for processing non-IID data, ensuring confidentiality, and algorithms for predicting burnout levels are discussed. Approaches to data coding, automated analysis, and identification of factors affecting psycho-emotional state are described, and the limitations of the study and directions for further development are outlined.

The "Conclusion" section shows how the federated learning architecture for analyzing students' psycho-emotional state on distributed confidential data is implemented and researched. It is considered that the adaptation of the FedAvg, FedOpt, and FedProx algorithms to the non-differentiable Random Forest Regression model ensures stable convergence of the global model in non-IID data conditions. The results confirm the practical applicability of federated learning in an educational environment while maintaining the confidentiality of information.

Author's Personal Contribution. All key results described in the dissertation were completed and compiled by the author. Furthermore, the author created the main research findings, analyses, models, and programs, and the conclusions were drawn based on the results obtained from the PhD student's work and research.

Structure and scope of work. The dissertation includes an introduction, five main chapters, a conclusion, and a list of references. The full dissertation is 144 pages long, including 46 illustrations and 14 tables. The bibliography contains 105 titles.