

**Г. У. БЕКТЕМЫСОВА^{1*}, Г. С. БАКИРОВА¹, Ш. Е. ЕРМУХАНБЕТОВА¹,
Г. А. ШЫНТОРЕ¹, Д. Б. УМУТКУЛОВ¹, Ж. С. МАНГЫШЕВА²**

¹Международный университет информационных технологий,
Алматы, Казахстан;

²Казахстанско-Британский технический университет, Алматы, Казахстан.
e-mail: *g.bektemisova@iitu.edu.kz, g.bakirova@iitu.edu.kz, s.yermukhanbetova@iitu.edu.kz,
g.shyntore@iitu.edu.kz, d.umutkulov@iitu.edu.kz, mangysheva.zhanar@gmail.com

АНАЛИЗ АКТУАЛЬНОСТИ И ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ФЕДЕРАТИВНОГО ОБУЧЕНИЯ

В данной статье рассматривается федеративное обучение (ФО) как инновационный подход к машинному обучению, отличный от традиционных методов. В обычном машинном обучении (МО) данные собираются на центральном сервере для обучения модели. Однако в случае с ФО модель обучения направляется к данным, распределенным по локальным устройствам, и обучение происходит прямо на этих устройствах. Кроме того, в статье рассматриваются методы и алгоритмы федеративного обучения, определены преимущества и реальные области применения федеративного обучения. ФО находит применение в различных сферах, включая работу с медицинскими данными и персональными данными клиентов в компаниях сферы продаж. Этот подход особенно ценен для обеспечения конфиденциальности данных и соблюдения приватности.

Ключевые слова: федеративное обучение, машинное обучение, локальные устройства, интернет вещей, искусственный интеллект.

**Г. У. БЕКТЕМЫСОВА^{1*}, Г. С. БАКИРОВА¹, Ш. Е. ЕРМУХАНБЕТОВА¹,
Г. А. ШЫНТОРЕ¹, Д. Б. УМУТКУЛОВ¹, Ж. С. МАНГЫШЕВА²**

¹Халықаралық ақпараттық технологиялар университеті, Алматы, Қазақстан;

²Қазақ-Британ техникалық университеті, Алматы, Қазақстан.
e-mail: *g.bektemisova@iitu.edu.kz, g.bakirova@iitu.edu.kz, s.yermukhanbetova@iitu.edu.kz,
g.shyntore@iitu.edu.kz, d.umutkulov@iitu.edu.kz, mangysheva.zhanar@gmail.com

ФЕДЕРАТИВТІ ОҚЫТУДЫ ҚОЛДАНУДЫҢ ӨЗЕКТІЛІГІ МЕН ПЕРСПЕКТИВАСЫН ТАЛДАУ

Бұл мақалада федералды оқыту (ФО) дәстүрлі әдістерден өзгеше машиналық оқытудың инновациялық тәсілі ретінде қарастырылады. Кәдімгі машиналық оқытуда (МО) деректер модельді оқыту үшін орталық серверде жиналады. Алайда, ФО жағдайында оқыту моделі жергілікті құрылғыларға бөлінген деректерге бағытталады және оқыту тікелей осы құрылғыларда жүреді. Сонымен қатар, мақалада Федеративті оқытудың әдістері мен алгоритмдері қарастырылады. Федеративті оқытудың артықшылықтары мен нақты қолданылуы анықталады. ФО әртүрлі салаларда, соның ішінде медициналық мәліметтермен және сату компанияларындағы клиенттердің жеке деректерімен жұмыс істеуді қолданады. Бұл тәсіл деректердің құпиялылығы мен құпиялылықты сақтау үшін өте маңызды.

Түйін сөздер: федеративті оқыту, машиналық оқыту, жергілікті құрылғылар, заттар интернеті, жасанды интеллект.

G. U. BEKTEMYSOVA^{1*}, G. S. BAKIROVA¹, SH., G. YERMUKHANBETOVA¹,
A. SHYNTORE¹, D. B. UMUTKULOV¹, ZH. S. MANGYSHEVA²

¹International Information Technology University, Almaty, Kazakhstan;

²Kazakh-British Technical University, Almaty, Kazakhstan.

e-mail: *g.bektemisova@iitu.edu.kz, g.bakirova@iitu.edu.kz, s.yermukhanbetova@iitu.edu.kz,
g.shyntore@iitu.edu.kz, d.umutkulov@iitu.edu.kz, mangysheva.zhanar@gmail.com

ANALYSIS OF THE RELEVANCE AND PROSPECTS OF APPLICATION OF FEDERATE TRAINING

This article examines federated learning (FOE) as an innovative approach to machine learning, different from traditional methods. In conventional machine learning (MO), data is collected on a central server to train the model. However, in the case of FO, the learning model is directed to data distributed across local devices, and learning takes place directly on these devices. In addition, the article discusses methods and algorithms of federated learning, identifies the advantages and real areas of application of federated learning. FO is used in various fields, including working with medical data and personal data of customers in sales companies. This approach is especially valuable for ensuring data confidentiality and privacy.

Key words: federated learning, machine learning, local devices, Internet of Things, artificial intelligence.

Введение. В современном информационном обществе объемы данных растут в геометрической прогрессии, открывая новые перспективы и вызовы для обработки и анализа информации. Однако с увеличением количества данных возникают проблемы с их централизованным хранением и обработкой, такие как уязвимость конфиденциальности и безопасности, а также неэффективное использование ресурсов.

В этом контексте федеративное обучение становится важным и перспективным направлением исследований в области машинного обучения. Федеративное обучение представляет собой подход, при котором модели обучаются на распределенных устройствах, не передавая при этом конфиденциальные данные на центральный сервер. Такой подход обеспечивает не только сохранность приватности данных, но и позволяет эффективно использовать ресурсы, распределенные по различным узлам сети.

В данной статье мы рассмотрим актуальность и перспективы применения федеративного обучения в различных сферах, начиная от медицинских приложений и финансовых сервисов до обеспечения кибербезопасности и управления городскими системами. Мы также проанализировали существующие подходы и решения в области федеративного обучения, выделив его преимущества, ограничения и возможности дальнейшего развития. Наша работа также охватывает перспективные направления исследований и практического применения федеративного обучения, а также вызовы, стоящие перед этим перспективным направлением в будущем.

Литературный обзор. Федеративное обучение (ФО) представляет собой инновационный подход к машинному обучению, который позволяет сохранять и обучать модели на локальных устройствах без централизованной передачи данных на сервер. Это способствует сохранению конфиденциальности данных, снижению затрат на передачу информации и решению проблем, связанных с централизованным хранением.

В рамках ФО глобальная модель хранится на центральном сервере, а копии модели передаются на локальные устройства для обучения на основе местных данных. Со временем модели на устройствах становятся более приватными. При обновлении параметров модели данные от локальных моделей передаются глобальной модели с использованием безопасных методов. Это позволяет объединять и усреднять данные для получения новых знаний, расширяя возможности модели за счет данных из различных источников.

Устаревшие методы сбора данных и централизованный подход к машинному обучению могут создавать проблемы безопасности и конфиденциальности. ФО представляет инновационные методы для снижения рисков и обеспечения безопасности и конфиденциальности при сборе информации.

В статье [1] рассматриваются потенциальные проблемы безопасности и конфиденциальности при использовании передовых технологий в "умных" городах, таких как рост использования искусственного интеллекта (ИИ) и Интернета вещей. Статья [2] обращает внимание на увеличивающуюся сложность управления данными и ресурсами из-за роста населения и объема передачи информации. В статье [3] подчеркивается важность исследований в сенсорном зондировании "умных" городов и рассматривается потенциал ФО в решении проблем конфиденциальности и безопасности при сборе данных.

Статья [4] обсуждает распространение Интернета вещей в различные сферы повседневной жизни благодаря следующим факторам: традиционные технологии искусственного интеллекта требуют централизованного сбора и обработки данных, что может быть невозможно в реальных сценариях применения из-за высокой масштабируемости современных сетей и возрастающих проблем с конфиденциальностью. Федеративное обучение представляет собой подход к распределенному совместному обучению искусственного интеллекта, который позволяет обучать модели на распределенных устройствах без обмена данными. Применение федеративного обучения включает "умное" здравоохранение, "умный" транспорт, "умные" города и "умные" отрасли.

В статье [5] проведен краткий анализ алгоритмов машинного обучения для обеспечения безопасности Интернета вещей с основным вниманием на реализации алгоритмов федеративного и глубокого обучения. Федеративное обучение позволяет сохранять конфиденциальность данных при обмене информацией с другими системами, преодолевая недостатки традиционных методов машинного обучения.

Статья [6] отмечает, что устаревшие модели сбора данных, основанные на централизованных подходах машинного обучения, сопровождаются проблемами конфиденциальности и безопасности. Для решения этих проблем предлагается использовать федеративное обучение. В статье представлен обзор систем зондирования "умных городов" и рассмотрен потенциал федеративного обучения в сборе данных.

В статье [7] сформулирован вывод о том, что с появлением новых технологий, таких как искусственный интеллект вещей, приложения для "умных городов" сталкиваются с проблемами утечки конфиденциальной информации. Для защиты конфиденциальности информации предлагается интегрировать совместное обучение с приложениями "умных городов".

Методы и методология. Алгоритмы федеративного обучения являются ключевым компонентом в системах, где данные распределены между несколькими устройствами или серверами, и цель состоит в обучении общей модели без необходимости централизованного сбора данных. Нами представлены некоторые из наиболее широко используемых алгоритмов федеративного обучения.

Алгоритм Federated Averaging (FedAvg) является одним из наиболее распространенных и простых в реализации методов федеративного обучения. Он предполагает, что каждое устройство обучается локально на своих данных, а затем параметры модели усредняются на центральном сервере. Математическое представление этого алгоритма:

1. Инициализация: начинаем с инициализации глобальной модели θ_0 случайными параметрами.

2. Федеративное обучение: для каждой эпохи t выполняем следующие шаги:

- Каждое устройство участник k выполняет локальное обучение на своих данных с использованием текущих параметров модели θ_t и возвращает обновленные параметры $\theta_{t,k}$
- Центральный сервер агрегирует полученные параметры от всех устройств участников и вычисляет среднее значение:

$$\bar{\theta}_t = \frac{1}{K} \sum_{k=1}^K \theta_{t,k}$$

- Глобальная модель θ_t обновляется с использованием среднего значения параметров:

$$\theta_{t,k} = \bar{\theta}_t$$

2. Повторение: Процесс повторяется до достижения заданного количества эпох или пока не будет достигнуто условие остановки.

Алгоритм Federated Learning with Differential Privacy (FedDP) включает в себя методы дифференциальной конфиденциальности, чтобы обеспечить защиту личных данных пользователей. Он добавляет шум к параметрам модели перед их передачей на центральный сервер.

Алгоритм Federated Learning with Secure Aggregation (FedSecAgg) предлагает методы шифрования и безопасной агрегации параметров модели для защиты данных в процессе передачи между устройствами и сервером.

Алгоритм Federated Learning with Split Learning (FedSplit) использует методы разделенного обучения для обеспечения безопасности и конфиденциальности данных. Вместо передачи сырых данных на центральный сервер, устройства передают промежуточные представления или признаки.

Алгоритм Federated Learning with Model Personalization (FedPer) позволяет каждому устройству персонализировать общую модель под свои уникальные данные, что позволяет получать более точные и адаптированные результаты для каждого устройства.

Эти алгоритмы и их вариации активно исследуются и разрабатываются в сфере федеративного обучения для обеспечения эффективного и безопасного обучения на распределенных данных.

Категоризация ФО. Нами были analyzed методы федеративного обучения, которые делятся на три группы: горизонтальное, вертикальное и федеративное трансферное обучение [7].

Горизонтальное федеративное обучение направлено на горизонтальную централизацию данных похожих устройств в пределах одного уровня или горизонта. Например, общие метки классов и примеры данных могут объединяться горизонтально. Обмен данных происходит между подобными устройствами, и обновленные модели передаются друг другу. Метод горизонтального федеративного обучения эффективен, когда общие шаблоны или закономерности могут быть извлечены из данных различных устройств. Это позволяет устройствам схожего типа обмениваться знаниями и учиться друг у друга, что может быть полезно, когда данные имеют общие характеристики [8]. Также этот метод позволяет решать технические и практические задачи путем распределения данных на различные устройства. Алгоритм сравнивает характеристики и связывает их соответствующим образом. Пример горизонтального федеративного обучения представлен на рисунке 1.

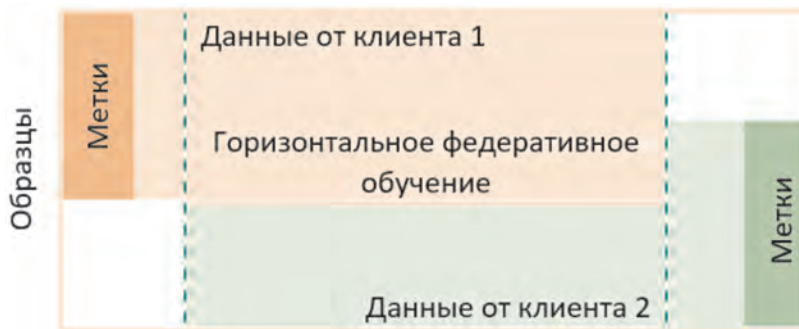


Рисунок 1 – Горизонтальное ФО

Одним из примеров горизонтального метода является его использование для предсказания поведения покупателей. Например, предположим, что необходимо предсказать эмоциональную окраску отзывов о продуктах. Для этого мы можем применить горизонтальное федеративное обучение с использованием мобильных устройств для обучения модели предсказывать эмоциональную окраску текстовых сообщений. Предположим, что каждое устройство (например, смартфон) обладает данными о текстовых отзывах пользователей, отправленных с этого устройства.

Алгоритм действия горизонтального ФО.

Шаг 1: Пользователь со смартфона 1 передает положительные отзывы, пользователь со смартфона 2 передает отрицательные отзывы, а пользователь со смартфона 3 передает как положительные, так и отрицательные отзывы. Обучение модели машинного обучения происходит на каждом устройстве, где модель предсказывает эмоциональный окрас текста, например, "положительный" или "отрицательный".

Шаг 2: После нескольких повторений обучения устройства обмениваются некоторыми параметрами моделей, чтобы каждая модель приобрела общее представление о данных с других устройств.

Шаг 3: Каждое устройство выполняет локальное обновление своей модели, используя информацию от других устройств. Например, устройство 1 может улучшить свою способность распознавать негативные тексты, основываясь на данных от устройства 2.

Шаг 4: Каждое устройство снова выполняет локальное обновление своей модели, используя информацию от других устройств. Например, устройство 1 может улучшить свою способность распознавать негативные тексты, основываясь на данных от устройства 2.

В итоге, после нескольких повторений обмена и локального обновления, устройства могут создать общую модель, которая обладает улучшенным предсказательным потенциалом для всех типов отзывов, даже несмотря на то, что каждое устройство изначально обучалось на данных своего пользователя.

Данный опыт показывает, как горизонтальное федеративное обучение позволяет устройствам схожих характеристик (в данном случае отправкой отзывов) обмениваться знаниями и улучшать общую модель, сохраняя при этом конфиденциальность личных данных пользователей.

Вертикальное федеративное обучение. Вертикальное федеративное обучение ориентировано на объединение вертикально разделенных данных, т.е. данных, разделенных по признакам или атрибутам. Обмен информацией происходит между устройствами, владеющими разными аспектами данных. Модели обучаются на этих частях данных, а затем объединяются для создания общей модели. Этот подход позволяет устройствам с различными характеристиками обмениваться знаниями, что может улучшить качество модели, особенно когда разные устройства содержат уникальные аспекты данных.

Например, предположим, у нас есть две организации: одна имеет данные о пациентах (например, их имена), а другая – медицинскую информацию (например, результаты анализов). Вертикальное федеративное обучение позволило бы этим организациям совместно обучать модель, не раскрывая конкретные имена пациентов и их медицинские результаты. Пример вертикального федеративного обучения представлен на рисунке 2.

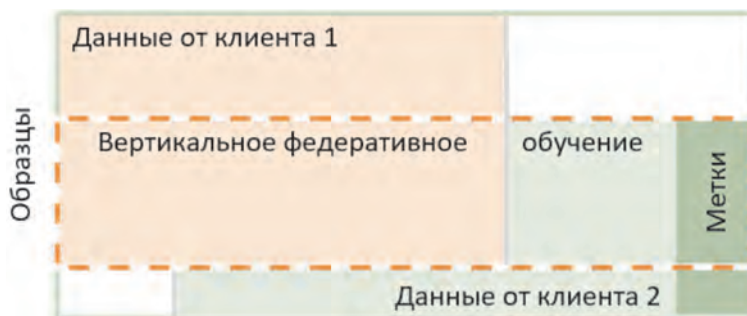


Рисунок 2 – Вертикальное ФО

Алгоритм действия вертикального обучения.

У организации 1 есть данные о именах пациентов, а у другой – данные об анализах. Каждая организация начинает обучение модели на своих локальных данных.

Однако они не могут полностью обучить модель, так как имеют доступ только к части всей информации. Организация 1 и Организация 2 делятся отдельно обученными статистиками или характеристиками, не раскрывая реальных данных о пациентах. Например, Организация 1 может отправить данные для каждой отдельной категории. Затем каждая организация обновляет свою модель, обрабатывая полученную информацию. Например, Организация 1, опираясь на данные Организации 2, может выставить более точный диагноз. После нескольких процессов обмена и локального обновления организации создают общую модель, которая учитывает как данные пациентов, так и результаты анализов, не раскрывая личные данные о пациентах. В итоге модель может ставить диагнозы на основе разнообразных характеристик

Федеративное трансферное обучение. Федеративное трансферное обучение отличается от сценариев горизонтального и вертикального федеративного обучения тем, что в большинстве случаев данные не разделяют ни пространство выборок, ни пространство признаков. Основная проблема заключается в отсутствии меток данных при их низком качестве. Знания из исходной области переносятся в целевую область для достижения лучших результатов обучения при трансферном обучении. Однако этот метод обеспечивает защиту данных и конфиденциальность пользователей[8].

Федеративное трансферное обучение используется для переобучения с одной модели на другую. Оно объединяет концепции федеративного обучения и трансферного обучения. Этот метод применяется, когда устройства обладают похожими характеристиками и уникальными данными, которые используются для обучения глобальной модели. Пример федеративного трансферного обучения представлен на рисунке 3.



Рисунок 3 – Федеративное трансферное обучение

Алгоритм действия федеративного трансферного обучения.

Рассмотрим на примере: на Гаджете 1 имеются данные о картинках типов растений, а на Гаджете 2 – о картинках различных видов зданий. Устройства начинают обучение модели для определения объектов на своих изображениях. Гаджет 1 и Гаджет 2 обмениваются одним из параметров своих моделей и некоторой обработанной информацией, защищая свои данные. Гаджет 1, применяя принятые параметры от Гаджета 2, реализует локальное трансферное обучение для улучшения способности модели распознавать здания. Аналогично Гаджет 2 применяет параметры от Гаджета 1 для улучшения способности модели распознавать растения. Глобальная модель

для распознавания как растений, так и зданий создается после нескольких операций обмена и локального трансферного обучения устройств. Устройства обмениваются знаниями и улучшают обобщающую способность модели.

Рассмотренный выше метод направлен на объединение данных устройств со схожими характеристиками, такими как тип данных или задача обучения. В отличие от горизонтального федеративного обучения, федеративное трансферное обучение учитывает общие шаблоны и закономерности, которые могут быть извлечены из данных различных устройств. Обмен знаний между подобными устройствами для улучшения обобщающей способности моделей является главной целью этого метода. Каждое устройство инициализирует свою модель для решения задачи обучения на основе собственных данных.

Преимущества федеративного обучения. В данной работе рассмотрены некоторые преимущества применения федеративного обучения (ФО). Эффективное использование данных позволяет объединить большой объем информации с различных устройств, что повышает качество глобальной модели и позволяет ей адаптироваться к различным сценариям. При этом данные хранятся на разных устройствах, таких как смартфоны, датчики Интернета вещей и другие. Личные данные локализуются на отдельных устройствах, что повышает конфиденциальность, особенно для таких организаций, как медицинские учреждения и др. Говоря о защите персональных данных, важно отметить, что они хранятся на устройствах, что обеспечивает их безопасность и снижает риск утечки данных. Кроме того, данные располагаются на устройствах, что обеспечивает легкий доступ к ним и не требует подключения к Интернету для обработки модели, что сокращает время выполнения задачи и расход трафика.

Реальные применения федеративного обучения. Также рассмотрены области применения федеративного обучения. Во-первых, смартфоны используются для предсказания слов, определения лиц при входе в систему и распознавания голоса с помощью Siri или Google Assistant. Во-вторых, автомобили с автопилотом используют данные для оценки окружающей среды и улучшения точности с помощью компьютерного зрения и машинного обучения. В-третьих, федеративное обучение улучшает системы прогнозирования продаж, опираясь на разнообразные данные для определения спроса на продукцию. В-четвертых, в области здравоохранения федеративное обучение применяется для обучения моделей с безопасным доступом к данным пациентов и обмена информацией между медицинскими организациями для обогащения набора данных и повышения безопасности обучения локальных моделей. Это позволяет медицинским работникам получать доступ к данным о пациентах и их заболеваниях из разных точек мира, а также позволяет медицинским учреждениям с небольшим количеством пациентов использовать новейшие возможности искусственного интеллекта.

Заключение. Федеративное обучение обеспечивает безопасность и конфиденциальность данных, ускоряет процесс обучения моделей и гарантирует безопасность данных после тренировки моделей для их распространения. Федеративное обучение становится все более популярным в различных отраслях, таких как здравоохранение, промышленность и электронная торговля.

Федеративное обучение позволяет создать точную глобальную модель, не требуя выноса данных с локальных устройств. Оно включает передачу моделей и параметров между сервером и локальными устройствами.

ЛИТЕРАТУРА

- 1 Xia L. , Semirumi D.T., Rezaeihttps R. (2023). A thorough examination of smart city applications Exploring challenges and solutions throughout the life cycle with emphasis on safeguarding citizen privacy. *Sustainable Cities and Society*, 98.
- 2 Joshua Stock, Oliver Hauke, , Julius Weißmann, Hannes Federrath. (2023). *The Applicability of Federated Learning to Official Statistics*. Cornell University.
- 3 Ji Chu Jiang 1, Burak Kantarci, Sema Oktug, Tolga Soyata. (2020) *Federated Learning in Smart City Sensing: Challenges and Opportunities*, Sensors.
- 4 Dinh C. Nguyen, Ming Ding, Pubudu N. Pathirana, Aruna Seneviratne, Jun Li, H. Vincent Poor. (2021). *Federated Learning for Internet of Things: A Comprehensive Survey*. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, VOL. 23, NO. 3.
- 5 Vinay Gugueoth, Sunitha Safavat, Sachin Shetty (2023). *Security of Internet of Things (IoT) using federated learning and deep learning – Recent advancements, issues and prospects*. *ICT Express*, Volume 9, Issue 5, Pages 941-960.
- 6 Ji Chu Jiang, Burak Kantarci, Sema Oktug, Tolga Soyata. (2020). *Federated Learning in Smart City Sensing: Challenges and Opportunities Sensors*, 20(21), 6230.
- 7 Sharnil Pandya a, Gautam Srivastava b i j, Rutvij Jhaveri c, M. Rajasekhara Babu d, Sweta Bhattacharya e, Praveen Kumar Reddy Maddikunta e, Spyridon Mastorakis g, Md. Jalil Piran h, Thippa Reddy Gadekallu. (2023). *Sustainable Energy Technologies and Assessments*. *Sustainable Energy Technologies and Assessments*, Volume 55.
- 8 Li, Li, Yuxi, Fan, Mike, Tse, Kuo-Yi, Lin. (2020). *A review of applications in federated learning*. *Computers & Industrial Engineering*, Volume 149.
- 9 A survey on security and privacy of federated learning, Viraaji Mothukuri a, Reza M. Parizi a, Seyedamin Pouriye h b, Yan Huang a, Ali Dehghantanha c, Gautam Srivastav.
- 10 Yang, Q.a , Liu, Y., Chen, T. and Tong, Y. (2019). *Federated Machine Learning: Concept and Applications*. *ACM Transactions on Intelligent Systems and Technology*, 10(2), 1–19.

REFERENCES

- 1 Xia L. , Semirumi D.T., Rezaeihttps R. (2023). A thorough examination of smart city applications Exploring challenges and solutions throughout the life cycle with emphasis on safeguarding citizen privacy. *Sustainable Cities and Society*, 98.
- 2 Joshua Stock, Oliver Hauke, , Julius Weißmann, Hannes Federrath. (2023). *The Applicability of Federated Learning to Official Statistics*. Cornell University.
- 3 Ji Chu Jiang 1, Burak Kantarci, Sema Oktug, Tolga Soyata. (2020) *Federated Learning in Smart City Sensing: Challenges and Opportunities*, Sensors.
- 4 Dinh C. Nguyen, Ming Ding, Pubudu N. Pathirana, Aruna Seneviratne, Jun Li, H. Vincent Poor. (2021). *Federated Learning for Internet of Things: A Comprehensive Survey*. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*, VOL. 23, NO. 3.
- 5 Vinay Gugueoth, Sunitha Safavat, Sachin Shetty (2023). *Security of Internet of Things (IoT) using federated learning and deep learning – Recent advancements, issues and prospects*. *ICT Express*, Volume 9, Issue 5, Pages 941-960.
- 6 Ji Chu Jiang, Burak Kantarci, Sema Oktug, Tolga Soyata. (2020). *Federated Learning in Smart City Sensing: Challenges and Opportunities Sensors*, 20(21), 6230.
- 7 Sharnil Pandya a, Gautam Srivastava b i j, Rutvij Jhaveri c, M. Rajasekhara Babu d, Sweta Bhattacharya e, Praveen Kumar Reddy Maddikunta e, Spyridon Mastorakis g, Md. Jalil Piran h, Thippa Reddy Gadekallu. (2023). *Sustainable Energy Technologies and Assessments*. *Sustainable Energy Technologies and Assessments*, Volume 55.

8 Li, Li, Yuxi, Fan, Mike, Tse, Kuo-Yi, Lin. (2020). A review of applications in federated learning. *Computers & Industrial Engineering*, Volume 149.

9 A survey on security and privacy of federated learning, Viraaji Mothukuri a, Reza M. Parizi a, Seyedamin Pouriyeh b, Yan Huang a, Ali Dehghantanha c, Gautam Srivastav.

10 Yang, Q.a , Liu, Y., Chen, T. and Tong, Y. (2019). Federated Machine Learning: Concept and Applications. *ACM Transactions on Intelligent Systems and Technology*, 10(2), 1–19.