ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ

УДК 004.89 Обзорная статья
DOI: 10.35330/1991-6639-2024-26-2-26-33
EDN: RTVEBB

Федеративное обучение для IoT и AIoT: применения, проблемы и перспективы

Х. М. Елеев

Научно-образовательный центр
Кабардино-Балкарского научного центра Российской академии наук
360010, Россия, г. Нальчик, ул. Балкарова, 2

Аннотация. В статье рассматривается концепция федеративного обучения (FL) – распределенного совместного подхода к искусственному интеллекту (AI), который позволяет обучать AI на распределенных IoT устройствах без необходимости обмена данными. Подходы и методы реализации FL для AIoT устройств были классифицированы по трем типам архитектуры федеративного обучения для организации взаимодействия между участниками обучения: централизованная, децентрализованная и гибридная. Рассмотрены подходы, основанные на различных технологиях, таких как Knowledge Distillation, блокчейн, беспроводные сети типа Mesh, Hybrid-IoT, DHA-FL. Для каждой рассмотренной технологии обозначены основные преимущества, проблемы и вызовы. В заключение сделаны выводы о перспективах развития FL для IoT и AIoT.

Ключевые слова: Интернет вещей (IoT), федеративное обучение (FL), искусственный интеллект вещей (AIoT), блокчейн, архитектура

Поступила 29.02.2024, одобрена после рецензирования 04.03.2024, принята к публикации 08.03.2024

Для цитирования. Елеев Х. М. Федеративное обучение для IoT и AIoT: применения, проблемы и перспективы // Известия Кабардино-Балкарского научного центра РАН. 2024. Т. 26. № 2. С. 26–33. DOI: 10.35330/1991-6639-2024-26-2-26-33

MSC: 68T99 Review article

Federated learning for IoT and AIoT: applications, challenges and perspectives

Kh.M. Eleev

Scientific and Educational Center
Kabardino-Balkarian Scientific Center of the Russian Academy of Sciences
360010, Russia, Nalchik, 2 Balkarov street

Abstract. This paper discusses the concept of federated learning (FL), a distributed collaborative approach to artificial intelligence (AI) that enables AI training on distributed IoT devices without need for data sharing. Approaches and methods for implementing FL for AIoT devices have been classified into three types of federated learning architecture for organizing interactions between learning participants, centralized, decentralized, and hybrid. Approaches based on different technologies such as Knowledge Distillation, blockchain, wireless networks like Mesh, Hybrid-IoT, DHA-FL are considered. For each technology considered, the main advantages, problems and challenges are outlined. The paper sums up with conclusions about the prospects of FL development for IoT and AIoT.

Keywords: Internet of things (IoT), federated learning (FL), artificial intelligence of things (AIoT), blockchain, architecture

Submitted 29.02.2024, approved after reviewing 04.03.2024, accepted for publication 08.03.2024

For citation. Eleev Kh.M. Federated learning for IoT and AIoT: applications, challenges and perspectives. *News of the Kabardino-Balkarian Scientific Center of RAS.* 2024. Vol. 26. No. 2. Pp. 26–33. DOI: 10.35330/1991-6639-2024-26-2-26-33

Введение

Стремительное развитие устройств Интернета вещей (Internet of things, IoT) приводит к росту объема данных, генерируемых такими устройствами. Они все больше и больше используются в домах людей, на производствах, в здравоохранении, собирая личную или чувствительную информацию о пользователях, такую как их местоположение, поведение, предпочтения, здоровье. Также классические облачные методы сбора и хранения информации становятся неэффективными из-за чрезвычайно высоких затрат на связь и расходов на хранение данных, собранных с миллионов или миллиардов устройств IoT.

Федеративное обучение позволяет обучать модели на данных, распределенных по разным устройствам, не требуя передачи этих данных на центральный сервер. Это может помочь в решении проблем конфиденциальности и безопасности, связанных с технологией IoT, так как данные остаются на устройствах пользователей и не раскрываются третьим сторонам. Такой подход не требует централизации данных, что может значительно сократить расходы на сбор и хранение информации.

1. Определение и характеристики AIoT, IoT и федеративного обучения

IoT – это сеть физических объектов, которые имеют встроенные датчики, контроллеры, актуаторы и средства связи, позволяющие им обмениваться данными и взаимодействовать друг с другом и с другими системами через интернет [1]. IoT позволяет расширить возможности компьютерных сетей за пределы традиционных устройств, таких как компьютеры, смартфоны и планшеты, и включить в них различные бытовые, промышленные и общественные объекты – лампочки, холодильники, машины, домофоны, датчики и т.д. IoT позволяет собирать большие объемы данных о состоянии и поведении объектов и окружающей среды, а также управлять ими удаленно и автоматически. В основе IoT лежит ряд ключевых концепций и технологий, включая идентификацию объектов (вещей) (например, IPv6), получение информации (например, RFID, датчики, GPS и т. д.), коммуникационные технологии для обмена данными и технологии сетевой интеграции [2].

Важно отметить, что устаревшие вычислительные и телекоммуникационные архитектуры не были разработаны с учетом особенностей IoT. Масштабы гетерогенных устройств, беспрецедентный объем, разнообразие и скорость данных в сочетании с чрезвычайной вариативностью контекста использования требуют новых парадигм в вычислениях [2].

В качестве такой парадигмы приходят искусственный интеллект (ИИ) и федеративное обучение.

Федеративное обучение (Federation Learning, FL) – это техника машинного обучения, которая позволяет обучать модели AI на децентрализованных данных, без необходимости централизовать или передавать эти данные. Это означает, что устройства, которые генерируют и хранят данные, могут обучать локальные модели AI на своих данных, а затем обме-

ниваться только параметрами или обновлениями моделей с центральным сервером или другими устройствами. Таким образом, создается общая глобальная модель AI, которая учитывает данные и знания всех участников [3].

Федеративное обучение обучает центральную модель с помощью децентрализованных данных без ущерба для конфиденциальности пользователей, благодаря этому она широко используется в устройствах IoT.

Результатом интеграции ИИ, в том числе федеративного обучения, с устройствами интернета вещей является AIoT (Artificial Intelligence of Things), что означает Искусственный Интеллект Вещей.

2. Обзор существующих подходов и методов реализации федеративного обучения для AIoT устройств

Существуют различные подходы и методы FL для AIoT или IoT устройств, которые далее будут классифицированы по типу архитектуры федеративного обучения, используемой для организации взаимодействия между участниками обучения.

2.1. Централизованная архитектура

Это архитектура, при которой существует один сервер, который координирует обучение и агрегацию моделей от устройств. Это наиболее простой и распространенный подход к FL, который использует алгоритм FedAvg или его вариации [4]. В этой архитектуре сервер инициирует обучение, выбирая случайное подмножество устройств, которые имеют достаточно данных и заряда батареи. Затем сервер отправляет им текущую глобальную модель и просит их обучить локальную модель на своих данных [5]. После этого устройства отправляют свои обновления моделей на сервер, который вычисляет среднее взвешенное этих обновлений и формирует новую глобальную модель. Этот процесс повторяется до достижения желаемого уровня точности или сходимости [6]. На рисунке 1 представлена данная архитектура.

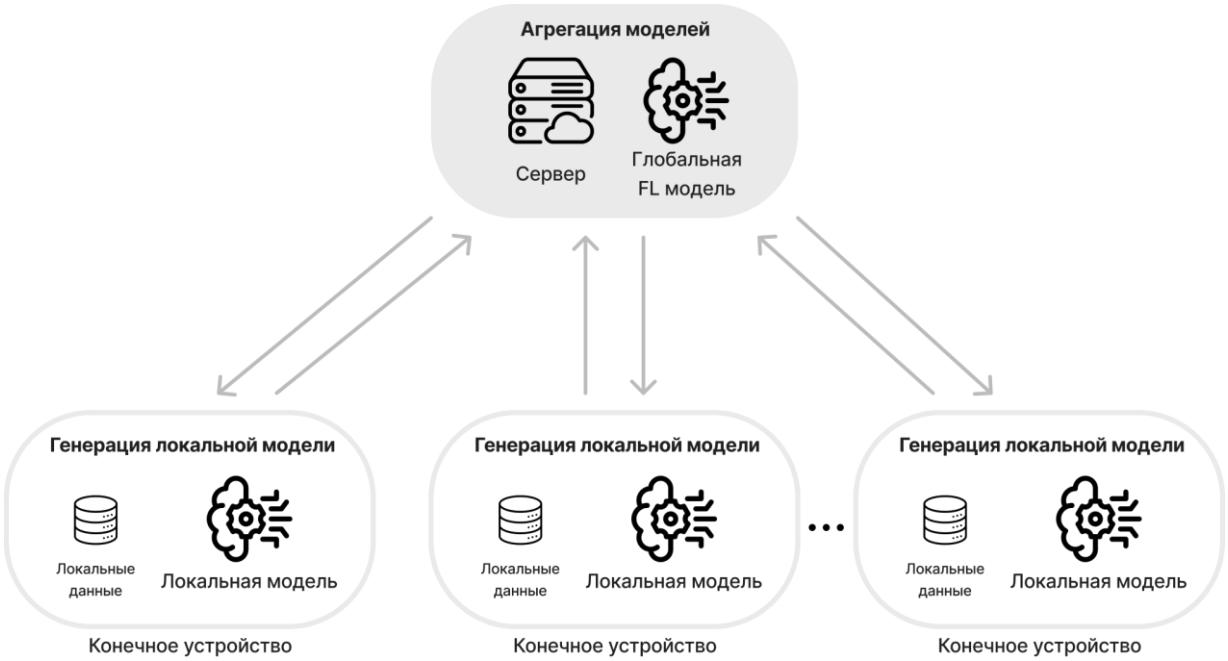

***Рис. 1**. Централизованная архитектура*

***Fig. 1.** Centralized architecture*

В статье [7] продемонстрирован подход, который использует Knowledge Distillation (KD). В этом подходе устройства обучают локальные модели на своих данных и отправляют на сервер не только градиенты моделей, но и мягкие цели (soft targets), которые представляют собой вероятности предсказаний для каждого класса. Сервер агрегирует градиенты и мягкие цели от устройств и формирует глобальную модель, которая затем распространяется на устройства для следующего раунда локального обучения. Во время локального обучения устройства используют как мягкие цели, так и жесткие метки (hard labels), которые представляют собой фактические классы для каждого образца, чтобы аппроксимировать предсказания модели. Это позволяет улучшить точность модели, используя дополнительную информацию от мягких целей. Авторы статьи также предлагают динамическую стратегию настройки весов функции потерь, которая позволяет оптимально согласовать мягкие цели и жесткие метки. Такой подход имеет ряд недостатков. Для передачи мягких целей, которые могут быть большими по размеру, требуется дополнительная коммуникация между устройствами и сервером, что может увеличить издержки на коммуникацию и потребление энергии, а также повысить риск утечки данных. Подход зависит от выбора весов функции потерь, которые определяют баланс между мягкими целями и жесткими метками. Это может быть сложной и эмпирической задачей, которая требует динамической настройки в зависимости от данных, моделей и сценариев применения.

В целом централизованная архитектура проста в реализации и координации, так как сервер контролирует все этапы обучения и агрегации моделей. Также такая архитектура показывает высокую точность и сходимость за счет центрального сервера, который может использовать все данные от устройств и оптимизировать глобальную модель. Но также центральный сервер несет в себе ряд проблем. Например, низкая масштабируемость и отказоустойчивость, так как сервер является узким местом и единой точкой отказа, которая может ограничивать производительность и надежность системы при увеличении числа устройств или данных [6]. Также сервер должен часто обмениваться большими объемами информации с устройствами, что может приводить к большим задержкам, потерям или перегрузкам сети [8].

2.2. Децентрализованная архитектура

При такой архитектуре нет центрального сервера, а устройства обмениваются информацией между собой через протоколы консенсуса, такие как блокчейн. Это более сложный и инновационный подход к FL, который использует алгоритмы, такие как FedCoin [9] или FedBC [10]. В этой архитектуре устройства самоорганизуются в децентрализованную сеть, в которой каждое устройство может выступать в роли клиента или сервера в зависимости от своего состояния и ресурсов. Устройства обучают локальные модели на своих данных и обмениваются обновлениями моделей с другими устройствами через блокчейн, который обеспечивает безопасность, прозрачность и неизменность транзакций [11]. Блокчейн также служит механизмом стимулирования устройств для участия в обучении и агрегации моделей [11]. Рисунок 2 демонстрирует данную архитектуру.

Помимо блокчейна, могут использоваться и другие методы реализации децентрализованной архитектуры. Например, авторы статьи [8] описывают подход, который использует беспроводную сеть типа mesh в качестве коммуникационной основы. В этом подходе устройства обучают локальные модели на своих данных и обмениваются обновлениями моделей с другими устройствами через протокол slotted ALOHA, который позволяет случайный доступ к каналу. Для минимизации размера модели на краю сети и снижения нагрузки

на коммуникацию используется передовая техника сжатия, основанная на генетических алгоритмах. Результаты симуляции показывают, что сжатая децентрализованная архитектура достигает производительности, сравнимой с базовой централизованной архитектурой и традиционным федеративным обучением с точки зрения точности и средней потери для задачи классификации. Такой подход требует высокой плотности и надежности устройств в сети, чтобы обеспечить достаточную связность и пропускную способность для обмена обновлениями моделей, что является недостатком.

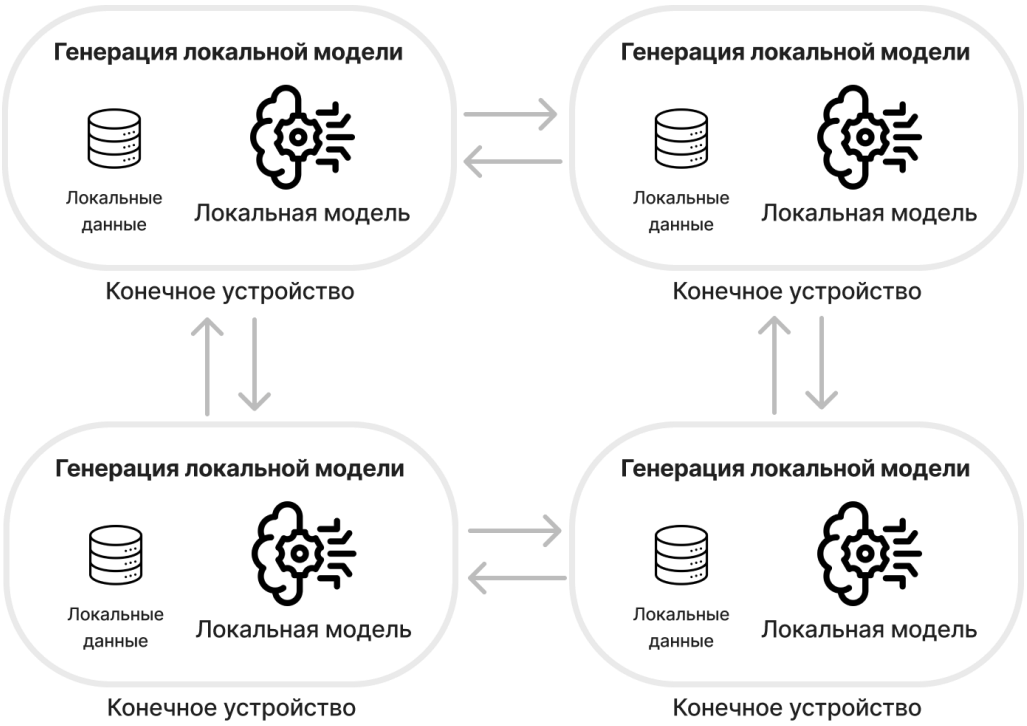

Рис. 2. *Децентрализованная архитектура*

Fig. 2. *Decentralized architecture*

Децентрализованная архитектура имеет высокую масштабируемость и отказоустойчивость, так как система не зависит от центрального сервера или облака, а может адаптироваться к динамическим изменениям в сети и устройствах. Задержки, потери и перегрузки сети снижены за счет того, что устройства обмениваются маленькими объемами информации с другими устройствами, а не с сервером [11]. Такая архитектура обеспечивает высокую гибкость и адаптивность, так как устройства могут использовать разные модели и алгоритмы для разных данных, вычислительных ресурсов или сценариев применения.

Такие системы требуют сложных алгоритмов и протоколов для обеспечения консенсуса, безопасности и стимулирования в децентрализованной сети [11], соответственно, сложны в реализации. Также система может страдать от проблем, таких как несбалансированность данных, несогласованность моделей, асинхронность обновлений или злонамеренные атаки, которые могут искажать или подрывать обучение, что снижает точность и сходимость. В случае реализации децентрализованной архитектуры с помощью технологии блокчейн, AIoT устройства должны выполнять дополнительные задачи, такие как шифрование, подпись, верификация или майнинг, что повышает потребность в вычислительных ресурсах.

2.3. Гибридная архитектура

Сочетает в себе элементы централизованной и децентрализованной архитектур, чтобы получить преимущества обоих подходов. В этой архитектуре устройства организуются в кластеры или подсети, в которых есть локальные серверы, которые координируют обучение и агрегацию моделей внутри кластера. Затем локальные серверы обмениваются информацией с глобальным сервером или другими локальными серверами через блокчейн или другие протоколы консенсуса, чтобы сформировать общую модель для всей системы. Пример такой архитектуры приведен на рисунке 3.

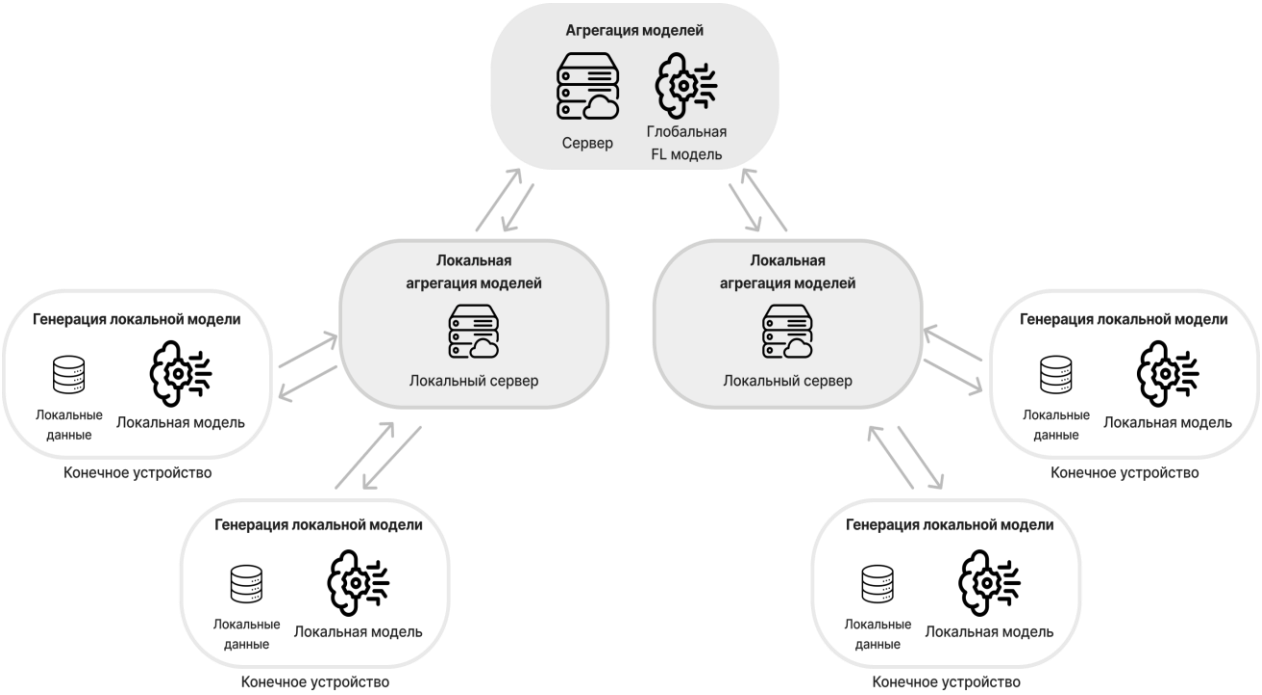

***Рис. 3**. Гибридная архитектура*

***Fig. 3.** Hybrid architecture*

Например, в данной статье [12] авторы демонстрируют гибридную блокчейн-архитектуру Hybrid-IoT. В Hybrid-IoT подгруппы IoT устройств становятся пирами на субблокчейнах PoW (Proof of Work) [13], соединенных межсетевой структурой BFT (Byzantine Fault Tolerant) с помощью фреймворка Polkadot или Cosmos. Она отлично демонстрирует эффективность гибридной архитектуры, которая может решить проблемы, связанные с конфиденциальностью, эффективностью и стимулированием данных, а также повышать масштабируемость, отказоустойчивость, гибкость и адаптивность системы. PoW, несмотря на высокую степень безопасности, также требует больших ресурсов и является менее энергоэффективным по сравнению с PoS (Proof of State) [14] и PoA (Proof of Authority) [14].

Также отличным примером реализации гибридной архитектуры является Decentralized Hierarchical Asynchronous Federated Learning (DHA-FL) [15]. DHA-FL использует иерархическую децентрализованную асинхронную архитектуру и обучает модели на краю сети, затем синхронизирует их с локальными или глобальными серверами без необходимости частой или большой коммуникации. Локальные серверы или серверы края в свою очередь асинхронно синхронизируют и агрегируют свои модели с другими локальными серверами, чтобы предотвратить отказы отдельных узлов и снизить влияние медленных устройств или отставших участников, что повышает устойчивость системы. DHA-FL также учитывает раз-

личия между устройствами в данных, ресурсах и сценариях применения и адаптирует модели и алгоритмы соответственно. Данный подход демонстрирует высокую скорость сходимости и точности. В свою очередь DHA-FL требует сложной координации между серверами на краю сети и устройствами AIoT, что может приводить к ошибкам синхронизации, потере данных или конфликтам версий моделей.

В свою очередь реализация гибридной архитектуры может столкнуться со сложностью координации и синхронизации между разными типами участников FL, которые могут иметь различные архитектуры моделей, протоколы коммуникации, частоты обновления и требования к конфиденциальности.

Заключение

Федеративное обучение для AIoT имеет большой потенциал для развития и применения в различных областях, таких как здравоохранение, транспорт, смарт-город, промышленность. Также данная технология может быть интегрирована с технологиями будущего для решения проблем таких технологий. Например, активно растущие 5G сети, которые представляют собой высокоскоростную связь с низкой задержкой для большого количества устройств, которые могут быть подвержены атакам или утечкам данных. AIoT устройства с технологией федеративного обучения способны решить эту проблему. Или новая и активно развивающаяся область метавселенных, которая гипотетически является следующим поколением сети Интернет, обеспечивающая полное подключение, погружение и вовлечение в онлайн с помощью устройств виртуальной и дополненной реальности. Связь между виртуальным и физическим миром обеспечивается данными, собранными с устройств IoT. Федеративное обучение – это перспективное решение для обеспечения взаимодействия между границами и сервером для повышения глобальной производительности, а также для повышения безопасности и конфиденциальности метавселенной [16].

REFERENCES

1. Khanna A., Kaur S. Internet of Things (IoT), Applications and challenges: a comprehensive review. *Wireless Personal Communications*. 2020. Vol. 114. Pp. 1687–1762. DOI: 10.1007/s11277-020-07446-4

2. Lynn Th., Takako E.P., Maria N.A. et al. The Internet of Things: definitions, key concepts, and reference architectures. *The Cloud-to-Thing*. 2020. Pp. 1–22. DOI: 10.1109/JIOT.2022.3229374

3. *Ефремов М. А., Холод И. И.* Разработка архитектуры универсального фреймворка федеративного обучения // Программные продукты и системы. 2022. Т. 35. №. 2. Pp. 263–272. DOI: 10.15827/0236-235X.138.263-272

Efremov M.A., Kholod I.I. Development of the architecture of a universal federated learning framework. *Programmnyye produkty i sistemy* [Software products and systems]. 2022. Vol. 35. No. 2. Pp. 263–272. DOI: 10.15827/0236-235X.138.263-272. (In Russian)

4. Latif U. Khan, Saad W., Han Z. et al. Federated learning for internet of things: recent advances, taxonomy, and open challenges. *IEEE Communications Surveys & Tutorials*. 2021. Vol. 23. No. 3. Pp. 1759–1799. DOI: 10.1109/COMST.2021.3090430

5. Sanchez-Iborra R. LPWAN and embedded machine learning as enablers for the next generation of wearable devices. *Sensors*. 2021. Vol. 21. No. 15. P. 5218. DOI: 10.3390/s21155218

6. Fan B., Jiang S., Su X., Hui P. Model-heterogeneous federated learning for internet of things: enabling technologies and future directions [Электронный ресурс]: *arXiv – CS – Distributed, Parallel and Cluster Computing*, 2023. URL: https://arxiv.org/pdf/2312.12091.pdf (дата обращения: 19.01.2024).

7. Liu T., Ling Z., Xia J. et al. Efficient federated learning for AIoT applications using knowledge distillation. *IEEE Internet of Things Journal*. 2023. Vol. 10. No. 8. Pp. 7229–7243. DOI: 10.1109/JIOT.2022.3229374

8. Salama A., Stergioulis A., Ali Zaidi S., McLernon D. Decentralized federated learning on the edge over wireless mesh networks. *IEEE Access*. 2023. Vol. 11. Pp. 124709–124724. DOI: 10.1109/ACCESS.2023.3329362

9. Liu Y., Ai Z., Sun S. et al. FedCoin: A Peer-to-peer payment system for federated learning [Электронный ресурс]: *arXiv*, 2023. URL: https://arxiv.org/pdf/2002.11711.pdf (дата обращения: 22 января, 2024).

10. Wu X., Wang Z., Zhao J. et al. FedBC: Blockchain-based decentralized federated learning. *IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA).* Dalian, 2020. Pp. 217–221. DOI: 10.1109/ICAICA50127.2020.9182705

11. Zhao Y., Zhao J., Jiang L. et al. Privacy-preserving blockchain-based federated learning for IoT device. *EEE Internet of Things Journal*. 2021. Vol. 8. No. 3. Pp. 1817–1829. DOI: 10.1109/JIOT.2020.3017377

12. Sagirlar G., Carminati B., Ferrari E. et al. Hybrid-IoT: Hybrid blockchain architecture for internet of things – PoW sub-blockchains. *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) / IEEE Computer Society*. Los Alamitos, 2018. Pp. 1007–1016. DOI: 10.1109/Cybermatics_2018.2018.00189

13. Gemeliarana I.G.A.K., Sari. R.F. Evaluation of proof of work (POW) blockchains security network on selfish mining. *International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*. Yogyakarta, 2018. Pp. 126–130. DOI: 10.1109/ISRITI.2018.8864381

14. Fahim S., Mahmood S., Katibur Rahman S.M. Blockchain: A Comparative study of consensus algorithms PoW, PoS, PoA, PoV. *International Journal of Mathematical Sciences and Computing (IJMSC)*. 2023. Vol. 9. No. 3. Pp. 46–57. DOI: 10.5815/ijmsc.2023.03.04

15. Houston Huff W., Balakrishnan R., Hao Feng et al. DHA-FL: Enabling efficient and effective AIoT via decentralized hierarchical asynchronous federated learning. *MLSys-RCLWN*, Miami, 2023.

16. Zhang T., Gao L., He C. et al. Federated learning for internet of things: applications, challenges, and opportunities. *IEEE Internet of Things Magazine*, 2022. Vol. 5. No. 1. Pp. 24–29. DOI: 10.1109/IOTM.004.2100182

Информация об авторе

Елеев Хазрат-Али Муратович, аспирант, Научно-образовательный центр Кабардино-Балкарского научного центра РАН;

360010, Россия, г. Нальчик, ул. Балкарова, 2;

khazratalieleev@gmail.com, ORCID: https://orcid.org/0009-0009-1536-7917

Information about the author

Hazrat-Ali M. Eleev, Post-graduate student, Scientific and Educational Center Kabardino-Balkarian Scientific Center of the Russian Academy of Sciences;

360010, Russia, Nalchik, 2 Balkarov street;

khazratalieleev@gmail.com, ORCID: https://orcid.org/0009-0009-1536-7917