BANGALORE INSTITUTE OF TECHNOLOGY

K.R. Road, V.V.Puram, Bengaluru-560 004

DEPARTMENT OF ARTIFICIAL INTELLIGENCE & MACHINE LEARNING

Project Work Synopsis

VII – SEM 2023-2024

PROJECT GROUP

Sl. No.	USN	NAME	Section	Email-Id	Phone No	Signature
1	1BI20AI022	Kollipara Sai Sandeep	A	ksai11122002@gmail.com	9059446766	
2	1BI20AI046	Shreyas R S	A	iamshrey26@gmail.com	8123516590	
3	1BI20AI048	Somula Jaswanth Reddy	A	jaswanthreddysomula@gmail.com	8688833274	
4	1BI20AI056	Vivek Pandith D V	A	vivekpanditdv@gmail.com	8296247974	

PROJECT DETAILS:

Title:	**Privacy Protected and Federated Adaptive Learning EdTech Platform**
Domain:	**Federated Learning**
Location:	**Bangalore**

For office use only:

Group ID:	
Guide:	
Status:	**Accepted/To be modified/Rejected**

Signature of the Project Co-Ordinator

PRIVACY PROTECTED AND FEDERATED ADAPTIVE LEARNING EdTECH PLATFORM

INTRODUCTION

In the ever-evolving landscape of education, the pursuit of personalized and effective learning experiences has taken centre stage. Our project "Privacy Protected and Federated Adaptive EdTech Learning Platform" encapsulates an ambitious vision to revolutionize education technology. Our aspiration to build this pioneering platform stems from a recognition of the urgent need for transformative change in the field of education.

This project seeks to establish a paradigm shift in educational technology, one that transcends traditional boundaries and unleashes the true potential of each student. Our vision revolves around the creation of an innovative, secure, and adaptable educational ecosystem that harnesses the power of technology to cater to the distinct learning profiles of every individual.

Traditional educational systems often adopt a one-size-fits-all approach, treating students as uniform entities rather than recognizing their unique strengths, weaknesses, and learning preferences. This approach not only limits the engagement and performance of students but also raises significant concerns regarding data privacy and security.

The "Privacy Protected and Federated Adaptive Learning EdTech Platform" aims to address these pressing challenges. By leveraging cutting-edge technologies, we endeavor to offer a learning environment that is dynamic and responsive to individual student performance. However, we are equally committed to upholding the highest standards of privacy and data security.

LITERATURE REVIEW

Chen Zhang's, Yu Xie b, Hang Bai, Bin Yu, Weihong Li a, Yuan Gao - [1] Survey on federated learning covers the decentralized collaborative approach where local devices perform training, sending model updates to a central aggregator, while preserving data privacy and addressing challenges in various aspects of the field.

Qi Xia, Winson Ye, Zeyi Tao, Jindi Wu, Qun Li - [2] survey on federated learning highlights its use for collaboratively training a shared prediction model across distributed nodes, emphasizing improved data privacy by keeping training data localized. The survey explores the challenges and considerations involved in implementing edge federated learning systems, including applications, development tools, communication efficiency, security, privacy, migration, and scheduling.

Tian Li, Anit Kumar Sahu, Ameet Talwalkar, and Virginia Smith - [3] Federated Learning presents unique challenges in heterogeneous and large-scale networks, necessitating innovative approaches for machine learning, distributed optimization, and privacy preservation. This article offers insights into the distinct features and obstacles of federated learning, surveys current methods, and suggests future research directions relevant to various research communities.

Hendra Kurniawan, and Masahiro Mambo - [4] This scheme integrates active learning with privacy protection through homomorphic encryption-based federated learning, enabling the selection of informative data while safeguarding sensitive labels. It effectively preserves privacy and reduces gradient leakage compared to alternative methods.

Jaehyoung Park, and Hyuk Lim - [5] The proposed Privacy-Preserving Federated Learning (PPFL) algorithm utilizes homomorphic encryption (HE) to protect local model parameters in a federated learning setup. It enables secure aggregation of encrypted model parameters on a centralized server while allowing different nodes to use distinct HE private keys within the same system, enhancing privacy in various cloud-based federated learning scenarios.

Stacey Truex, Georgia Nathalie Baracaldo - [6] Introduced a novel federated learning approach that combines differential privacy and secure multiparty computation (SMC) to address privacy and accuracy trade-offs. By doing so, it mitigates inference threats while maintaining high model accuracy, making it a scalable and effective solution for various machine learning models, outperforming existing state-of-the-art methods in experiments.

Antonio Muñoz, Ruben Ríos, Rodrigo Román, Javier López - [7] Underscores the importance of safeguarding personal devices in the face of growing security and privacy threats. It focuses on ARM TrustZone (TZ), a widely used technology in embedded devices like smartphones, and highlights vulnerabilities that have been exploited in the past. The paper offers insights into these vulnerabilities and suggests countermeasures while also presenting future challenges and open research areas in this domain.

Wei Ou, Jianhuan Zeng, Zijun Guo, Wanqin Yan, Dingwan Liu, and Stelios Fuentes - [8] Addresses the growing tension between data sharing and user data privacy in the era of AI and big data. It presents a vertical federated learning system for Bayesian machine learning with homomorphic encryption, allowing for model training without sharing raw data. The system achieves comparable model performance (up to 90%) to a centralized server while ensuring user privacy, making it applicable in various domains such as risk control, healthcare, finance, education, and data integration, thus helping to bridge data silos and safeguard user privacy.

Xiaoyuan Liu1, Hongwei Li1, Guowen Xu1, Rongxing Lu, Miao He - [9] Presented APFL, an Adaptive Privacy-preserving Federated Learning framework, which uses relevance propagation and adaptive noise injection to optimize the balance between privacy and accuracy in federated deep learning. Extensive experiments confirm APFL's superior performance in terms of accuracy, computation, and communication overhead.

Shiqiang Wang, Kin K. Leung - [10] Tackled the distributed machine learning at the network edge, presenting an algorithm that balances local updates and global parameter aggregation to optimize model training while conserving resources and preserving privacy. Extensive experiments validate its effectiveness across different machine learning models and data distributions.

Weizhao Jin, Yuhang Yao, Shanshan Han, Srivatsan Ravi - [11] introduces FedML-HE, a practical system for privacy-preserving Federated Learning (FL) using Homomorphic Encryption (HE). It significantly reduces overhead, making HE-based FL feasible for large models and scalable deployment on edge devices. The authors employ a novel universal overhead optimization scheme and demonstrate substantial overhead reduction, such as ~10x for ResNet-50 and ~40x for BERT models, enhancing FL's efficiency and privacy protection.

Rezak Aziz, Soumya Banerjee, Samia Bouzefrane 1 and Thinh Le Vinh -[12] Top analytics firms predict that by 2024, 75% of the global population will be covered by privacy regulations, emphasizing the need for robust security measures in next-generation internet environments. While Federated Learning (FL) is a promising method for collaborative model training without data sharing, recent studies reveal privacy vulnerabilities. This paper discusses privacy attacks on FL and explores Homomorphic Encryption (HE) and Differential Privacy (DP) as solutions. HE enables secure computations on encrypted data, while DP adds noise for privacy.

Michael Lahzi Gaid and Said A. Salloum -[13] Homomorphic Encryption, conceived in 1978 and realized by Craig Gentry in 2009, enables computations on encrypted data without the need for a secret key. The outcome remains encrypted and can be revealed later by the key owner. It's used for secure computation on ciphertexts, allowing privacy-preserving large-scale statistical analysis, especially in data encryption for high-security documents, including government applications.

Qiong Wu , Kaiwen He and Xu Chen -[14] The widespread adoption of the Internet of Things (IoT) has given rise to various intelligent IoT services and applications. Federated learning, designed to train a global model while preserving data privacy on IoT devices, faces challenges due to IoT's inherent device, statistical, and model heterogeneities. This paper proposes a personalized federated learning framework within a cloud-edge architecture for intelligent IoT applications. It explores personalized federated learning methods to address IoT heterogeneity and leverages edge computing for fast processing and low latency.

Nguyen Truong a , Kai Suna , Siyao Wang a , Florian Guittona , YiKe Guo- [15] Amid the rise of Machine Learning (ML)-based applications, data privacy and security have become imperative. ML service providers face challenges in data collection, management, and compliance with strict regulations like GDPR. Traditional centralized ML poses privacy risks. Federated Learning (FL) offers a solution by enabling collaborative learning without sharing data. However, FL's model parameter exchange raises privacy concerns and challenges GDPR compliance. This article surveys privacy-preserving techniques in FL concerning GDPR requirements and explores approaches to align FL systems with GDPR guidelines for full compliance.

Haokun Fang and Quan Qian- [16] This paper introduces PFMLP, a multi-party privacy-preserving machine learning framework that combines partially homomorphic encryption and federated learning. PFMLP enables learning parties to transmit encrypted gradients, preserving privacy. Experimental results show that PFMLP achieves nearly identical model accuracy with less than a 1% deviation. To mitigate computational overhead, an enhanced Paillier algorithm speeds up training by 25–28%. The paper also discusses encryption key length, learning network structure, and the number of learning clients in-depth for comprehensive comparisons.

Ayesha Manzur -[17] First proposed by Google, federated learning is described as an alternative to centralized artificial intelligence (AI) training where a shared universal model is trained under the coordination of a central server, from a combination of participating devices. The various devices in this model can add to the model’s training and knowledge and simultaneously keep most of the data in the device.

Tuo Zhang, Lei Gao, Chaoyang He, Mi Zhang, Bhaskar Krishnamachari, and Salman Avestimehr -[18] The proliferation of IoT devices, driven by faster Internet speeds and the advent of 5G/6G, will generate vast amounts of data containing users' private information. This data explosion, coupled with communication and storage costs and privacy concerns, challenges the traditional centralized over-the-cloud learning model. Federated Learning (FL) emerges as a promising alternative, enabling collaborative model training across multiple clients without centralizing data, reducing costs, and enhancing user privacy. However, challenges persist in implementing FL on IoT networks. This paper explores FL's opportunities and challenges in IoT platforms, discussing seven critical challenges and recent approaches to addressing them, thus enabling diverse IoT applications.

Alexander Brecko , Erik Kajati, Jiri Koziorek and Iveta Zolotova -[19] This paper discusses the deployment of AI and machine learning on edge devices, emphasizing the use of Federated Learning (FL) for creating global models from decentralized edge clients. FL offers advantages like scalability and data privacy but presents challenges, especially with heterogeneous devices in the Internet of Things (IoT). The paper provides an overview of FL methods, popular frameworks, and their communication mechanisms.

Jaehyoung Park 1 and Hyuk Lim-[20] Federated learning (FL) enables collaborative model training without sharing raw data, enhancing privacy. However, it faces risks of information inference from local models. This paper introduces Privacy-Preserving Federated Learning (PPFL) with homomorphic encryption (HE) to protect model parameters. PPFL allows the centralized server to aggregate encrypted local models without decryption. It also supports distributed cryptosystems, allowing nodes to use different HE private keys within the same FL system. The proposed PPFL algorithm is evaluated in various cloud-based FL service scenarios for performance analysis.

EXISTING SYSTEMS AND THEIR DRAWBACKS

Existing Systems:

- **Traditional Learning Environments:** Many educational institutions still rely heavily on traditional classroom-based learning. While this approach has its merits, it often lacks adaptability to individual student needs. The one-size-fits-all model may not cater to diverse learning styles and paces.
- **LMS (Learning Management Systems):** Learning Management Systems are widely used in both traditional and online education. These platforms offer content delivery, assessments, and tracking tools. However, they can be rigid in terms of personalization, and the user interfaces may not always be intuitive.
- **Online Courses and MOOCs:** Massive Open Online Courses (MOOCs) have gained popularity for providing accessible education. However, they can lack personalized interaction and often have low completion rates due to a lack of engagement.

Drawbacks of Existing Systems:

- **Limited Personalization:** Traditional systems often struggle to provide personalized learning experiences. Students with different abilities and learning styles may not receive the tailored support they need to excel.
- **Privacy Concerns:** In many online systems, especially MOOCs and LMS platforms, concerns exist about data privacy. Student data, including personal information and learning data, may be at risk of misuse or security breaches.
- **Engagement Issues:** Maintaining student engagement in online environments can be challenging. Passive content delivery and a lack of interactive features can lead to decreased motivation and learning outcomes.
- **Lack of Real-time Adaptation:** Most existing systems lack the ability to adapt to student performance in real time. This means that struggling students may not receive timely interventions, and advanced students may be held back.
- **Limited Data Utilization:** While data is often collected, its utilization for actionable insights is underutilized. Educators, students, and parents may not benefit fully from the potential insights offered by data analytics.

PROBLEM STATEMENT

The "Privacy Protected Federated Adaptive Learning Platform" project squarely confronts a formidable challenge within the realm of education technology. Traditional educational platforms have long been marred by their inability to deliver tailored learning experiences that account for the unique abilities and learning styles of each student. This one-size-fits-all approach not only fails to optimize student engagement and outcomes but also exposes sensitive user data to potential security breaches.

The central problem we address is the absence of a comprehensive educational solution that is both secure and adaptive. Existing platforms often fall short in terms of data privacy and security, limiting their effectiveness in delivering personalized learning experiences. The risk of data breaches and privacy infringements looms large, eroding trust and impeding progress in the educational technology sector.

Our project represents a pioneering effort to tackle these issues head-on. By incorporating federated learning, advanced encryption techniques, and secure execution environments, we aim to create a learning platform that continuously adapts to individual student performance while safeguarding the privacy and integrity of their data. Our goal is nothing short of redefining education technology, ensuring that every student can access a tailored and secure learning environment that empowers them to reach their full potential.
Key elements of our approach include:

- **Personalization:** Tailoring learning experiences to individual students.
- **Privacy Protection:** Utilizing advanced encryption techniques, federated learning, and secure environments.
- **Adaptive Ecosystem:** Creating a platform that adapts to student performance.
- **Data-Driven Insights:** Leveraging data to empower students, educators, and parents.
- **User-Friendly Interface:** Designing a frontend for intuitive and engaging learning experiences.

OBJECTIVES

1. **Decentralized Learning**: Implement a decentralized learning algorithm that allows individual learning agents to train models on their local data without sharing it with a central server. This preserves the privacy of the data while still allowing for collaborative learning.
2. **Adaptive Training Models**: Develop adaptive training models that can learn and improve over time based on new data and feedback from the learning agents. This ensures that the models stay relevant and effective as the data evolves.
3. **Cloud Server Learning**: Utilize cloud server learning to aggregate and analyze the model updates from the learning agents. This allows for global optimization of the model based on insights from all agents.
4. **Encrypted Communication**: Ensure secure and encrypted communication between the learning agents and the cloud server. This protects the privacy and integrity of the model updates during transmission.
5. **Adaptive edtech Platform**: Create an adaptive edtech platform that can dynamically adjust to changes in the ensemble model results. This allows for more efficient use of resources and better performance of the platform.
6. **Efficient Resource Utilization**: Design the system to make efficient use of computational and network resources. This could involve optimizing the timing and size of model updates to minimize network traffic.
7. **Personalized Learning Experience**: Aim to provide a personalized learning experience for each user by training models on their local data. This could improve the effectiveness of the learning platform.
8. **Privacy-Preserving Machine Learning:** Implement privacy-preserving machine learning algorithms that allow the models to learn from data without actually seeing it. This could be a key selling point for users who are concerned about privacy.
9. **Fairness**: Ensure fairness in learning so that all agents, regardless of the amount of local data they have, can benefit from the global model.

SOFTWARE REQUIREMENTS SPECIFICATION

Functional Requirements:

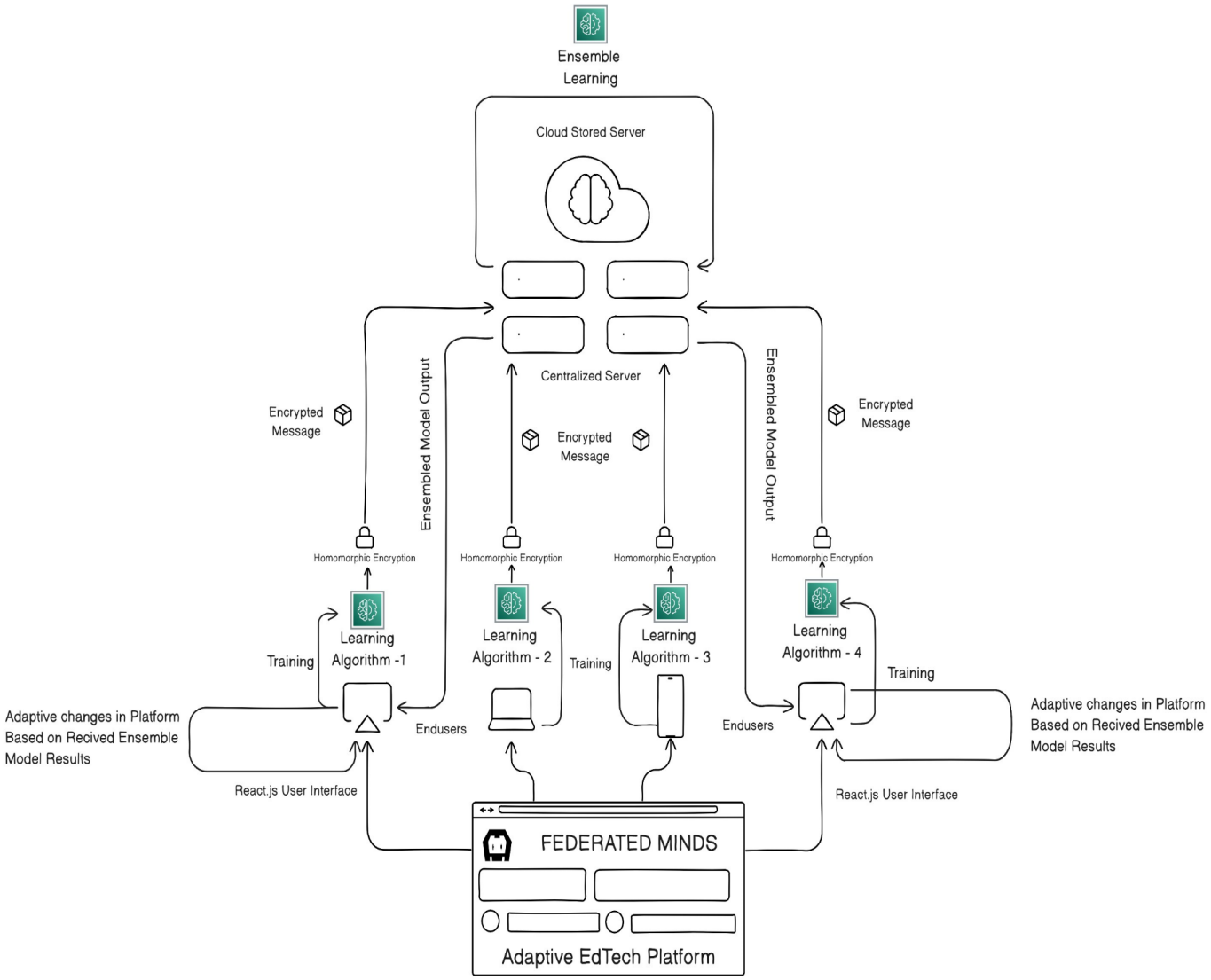
1. **User Registration and Authentication:** Users must be able to register for the platform using valid email addresses or other authorized credentials. Users should also authenticate securely using a combination of usernames and passwords or multi-factor authentication (MFA).
2. **User Profile Management:**Users should be able to create, edit, and manage their profiles, including personal information, educational history, and preferences.
3. **Educational Content Delivery:** The platform should provide educational content such as text, videos, quizzes, and assignments. Content must be categorized by subjects, topics, and difficulty levels.
4. **Personalized Recommendations:**The system should deliver personalized content recommendations based on user profiles, learning history, and performance data. Recommendations should adapt to individual learning styles and needs.
5. **Assessment and Progress Tracking:**Users should have access to quizzes, tests, and assessments. The platform should track user progress, provide feedback, and record assessment results.

6. **Federated Learning Integration:** Implement federated learning algorithms to enable decentralized model training. Edge devices should perform local model training and contribute updates to a central cloud server.
7. **Privacy Preservation:** Ensure that user data remains private and anonymous during federated learning processes. Implement differential privacy mechanisms to protect individual user information.
8. **Secure Communication:**Utilize secure communication protocols (e.g., TLS/SSL) to protect data transmitted between edge devices and the cloud server.
9. **User Interface (UI):**Develop user-friendly interfaces for students, teachers, and administrators to interact with the system. Ensure intuitive navigation and accessibility.
10. **Reporting and Analytics:**Provide reporting tools for teachers and administrators to track student performance and engagement. Generate analytics and insights from federated learning data.

Non-Functional Requirements:

1. **Security:**Ensure data security and privacy through encryption, secure user authentication, and secure data storage. Implement security measures to protect against unauthorized access and data breaches.
2. **Scalability:** Design the system to handle a growing number of users, edge devices, and educational content.Ensure that federated learning can scale as the number of edge devices increases.
3. **Performance:**The platform should deliver responsive user experiences with minimal latency. Federated learning training sessions should be efficient and resource-friendly on EndUser Devices.
4. **Reliability:** Maintain high system uptime and availability to support uninterrupted learning experiences.Implement backup and recovery mechanisms to handle system failures.
5. **Compatibility:**Ensure cross-device and cross-browser compatibility for user interfaces. Support various Raspberry Pi models and configurations.
6. **Regulatory Compliance:**Adhere to data privacy and security regulations, such as GDPR, COPPA, or any relevant local regulations. Ensure compliance with educational standards and requirements.
7. **Documentation:**Provide comprehensive documentation for administrators, developers, and end-users. Include user guides, system architecture documentation, and code documentation.
8. **Usability:**Design user interfaces with a focus on usability and accessibility, catering to users with diverse needs and abilities.
9. **Load Testing:**Conduct load testing to ensure the platform can handle concurrent users and federated learning sessions efficiently.
10. **Monitoring and Logging:**Implement robust monitoring and logging mechanisms to track system performance, errors, and security incidents. Set up alerts for system administrators.

BLOCK DIAGRAM / ARCHITECTURE



MODULE DESCRIPTION

- **Cloud Server:**

  The Cloud server acts as a centralized entity which collects all the encrypted individual weights from the edge devices and ensembles to get the best result. The Edge devices infer from this central model whenever necessary.

- **Edge Devices:**

  The edge devices are the main entities which draw a line between the traditional Machine Learning and Federated Learning. In FL, some part of the training happens at the edge devices. Hence, the load on the central server is reduced. The communication between the Server and Edge devices happens in an encrypted manner, in order to protect the privacy of the users.

- **Encryption:**

  Homomorphic encryption plays a crucial role in Federated Learning by allowing data to be securely aggregated and analyzed without exposing sensitive information, thereby preserving privacy in collaborative machine learning settings.

- **User Interface:**

  The User Interface gives us a Graphical Interface to communicate with the System. Users with different access types will be able to view the system from different aspects. Predominantly, ReactJS will be used for this purpose.

APPLICATIONS

1. **Personalized Learning:**

   By employing federated learning, educational institutions and EdTech companies can collaborate to improve recommendation systems and personalized learning experiences without sharing sensitive student data directly. This ensures that each student's privacy is maintained while still benefiting from a more tailored and effective educational experience.

2. **Healthcare Analytics:**

   Federated learning enables healthcare institutions to collaboratively train predictive models on patient data from various edge devices (like wearables and IoT sensors) and centralized cloud servers. Privacy is maintained, ensuring compliance with healthcare regulations while still improving diagnostic accuracy and treatment recommendations.

3. **Financial Fraud Detection:**

   Financial institutions can collaborate using federated learning to build better fraud detection models. Each institution can keep its customer transaction data confidential while contributing to the collective knowledge, leading to more accurate and timely fraud detection.

4. **Autonomous Vehicles:**

   Privacy-protected federated learning can be applied to autonomous vehicle systems. Car manufacturers and software developers can collaborate to improve self-driving algorithms by training on data collected from various vehicles on the road. Personal information about drivers and passengers is protected, while the overall safety and performance of autonomous systems are enhanced.

5. **Smart Cities:**

   In smart city deployments, federated learning can be used to analyze data from heterogeneous sources such as traffic cameras, environmental sensors, and citizen smartphones. This allows for real-time traffic management, pollution control, and public safety improvements without compromising individual privacy.

REFERENCES

[1] Chen Zhang, Yu Xie, Hang Bai, Bin Yu, Weihong Li, Yuan Gao, A survey on federated learning, Knowledge-Based Systems, Volume 216, 2021, 106775, ISSN 0950-7051, https://doi.org/10.1016/j.knosys.2021.106775.

[2] Xia, Q., Ye, W., Tao, Z., Wu, J. and Li, Q., 2021. A survey of federated learning for edge computing: Research problems and solutions. High-Confidence Computing, 1(1), p.100008.

[3] Li, T., Sahu, A.K., Talwalkar, A. and Smith, V., 2020. Federated learning: Challenges, methods, and future directions. IEEE signal processing magazine, 37(3), pp.50-60.

[4] Kurniawan, H. and Mambo, M., 2022. Homomorphic Encryption-Based Federated Privacy Preservation for Deep Active Learning. Entropy, 24(11), p.1545.

[5] Park, J. and Lim, H., 2022. Privacy-preserving federated learning using homomorphic encryption. Applied Sciences, 12(2), p.734.

[6] Truex, S., Baracaldo, N., Anwar, A., Steinke, T., Ludwig, H., Zhang, R. and Zhou, Y., 2019, November. A hybrid approach to privacy-preserving federated learning. In Proceedings of the 12th ACM workshop on artificial intelligence and security (pp. 1-11).

[7] Muñoz, A., Ríos, R., Román, R. and López, J., 2023. A survey on the (in) security of trusted execution environments. Computers & Security, 129, p.103180.

[8] Ou, W., Zeng, J., Guo, Z., Yan, W., Liu, D. and Fuentes, S., 2020. A homomorphic-encryption-based vertical federated learning scheme for rick management. Computer Science and Information Systems, 17(3), pp.819-834.

[9] Liu, X., Li, H., Xu, G., Lu, R. and He, M., 2020. Adaptive privacy-preserving federated learning. Peer-to-peer networking and applications, 13, pp.2356-2366.

[10] Wang, S., Tuor, T., Salonidis, T., Leung, K.K., Makaya, C., He, T. and Chan, K., 2019. Adaptive federated learning in resource constrained edge computing systems. IEEE journal on selected areas in communications, 37(6), pp.1205-1221.

[11] Jin, W., Yao, Y., Han, S., Joe-Wong, C., Ravi, S., Avestimehr, S. and He, C., 2023. FedML-HE: An Efficient Homomorphic-Encryption-Based Privacy-Preserving Federated Learning System. arXiv preprint arXiv:2303.10837.

[12] Aziz, R., Banerjee, S., Bouzefrane, S. and Le Vinh, T., 2023. Exploring Homomorphic Encryption and Differential Privacy Techniques towards Secure Federated Learning Paradigm. Future internet, 15(9), p.310.

[13] Gaid, M.L. and Salloum, S.A., 2021, May. Homomorphic encryption. In The International Conference on Artificial Intelligence and Computer Vision (pp. 634-642). Cham: Springer International Publishing.

[14] Wu, Q., He, K. and Chen, X., 2020. Personalized federated learning for intelligent IoT applications: A cloud-edge based framework. IEEE Open Journal of the Computer Society, 1, pp.35-44.

[15] Truong, N., Sun, K., Wang, S., Guitton, F. and Guo, Y., 2021. Privacy preservation in federated learning: An insightful survey from the GDPR perspective. Computers & Security, 110, p.102402.

[16] Fang, H. and Qian, Q., 2021. Privacy preserving machine learning with homomorphic encryption and federated learning. Future Internet, 13(4), p.94.

[17] Manzur, A., Federated Learning on Raspberry Pi. Medium article. https://medium.com/@ayeshamanzur123/federated-learning-on-raspberry-pi-8c470cfe7cd3

[18] Zhang, T., Gao, L., He, C., Zhang, M., Krishnamachari, B. and Avestimehr, A.S., 2022. Federated learning for the internet of things: Applications, challenges, and opportunities. IEEE Internet of Things Magazine, 5(1), pp.24-29.

[19] Brecko, A., Kajati, E., Koziorek, J. and Zolotova, I., 2022. Federated learning for edge computing: A survey. Applied Sciences, 12(18), p.9124.

[20] Park, J., Yu, N.Y. and Lim, H., 2022, October. Privacy-Preserving Federated Learning Using Homomorphic Encryption With Different Encryption Keys. In 2022 13th International Conference on Information and Communication Technology Convergence (ICTC) (pp. 1869-1871). IEEE.

[21] https://medium.com/@ayeshamanzur123/federated-learning-on-raspberry-pi-8c470cfe7cd3