International Journal of Open Publication and Exploration (IJOPE), ISSN: ISSN: 3006-2853
Volume 7, Issue 1, January-June, 2019, Available online at: https://ijope.com

Secure Federated Learning Framework for Distributed Ai Model Training in Cloud Environments

Rahul Saoji[1], Savita Nuguri[2], Krishnateja Shiva[3], Pradeep Etikani[4], Vijaya Venkata Sri Rama Bhaskar[5]

[1,2,3,4,5]Independent Researcher, USA

ABSTRACT

A new design for a secure FL solution that can be used for AI model training across many cloud services. The framework built in this paper is founded on federated learning which only involved the model and not the raw data of the organizations involved. These are federated model training pipelines, methods and approaches of privacy-preserving model updates, and differential privacy and identity and access management.

In this framework the issues of leakage of data, privacy violation and invasion by a nasty attacker is also addressed apart from the issues to do with legal matters. Thus, with the help of cloud environment integration and the availability of various data types, the proposed framework allows the improvement of the AI model performance and generation of the models that are closer to real-world while taking into consideration the data sovereignty and privacy concerns.

INTRODUCTION

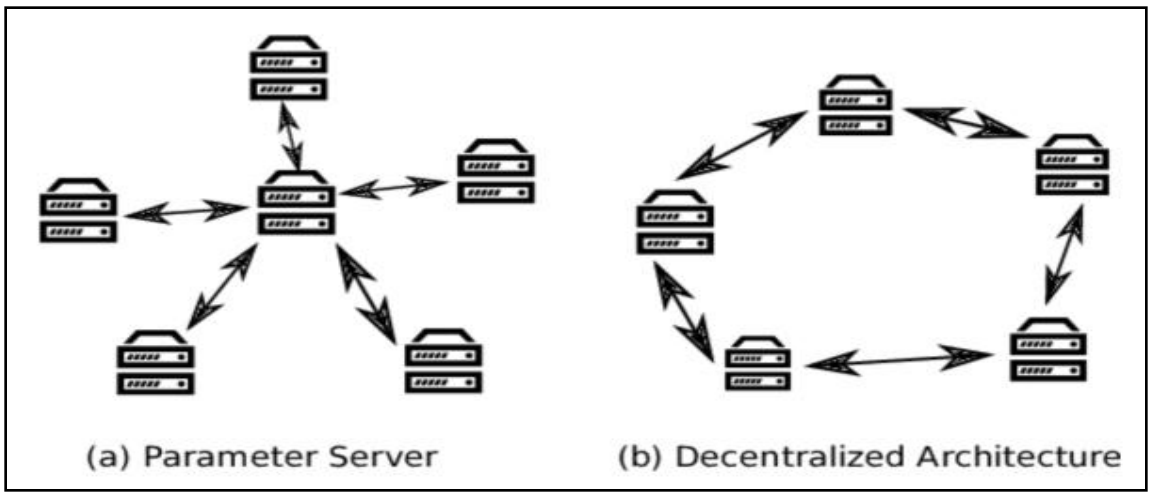
The training of artificial intelligence (AI) models is growing more challenging and demanding in terms of data and thus more diverse and collaborative. The main approach, which is also used in distributed model training, to compile data from many sources to a single point becomes problematic in the aspects of data privacy, data size and regulatory compliance. The three aforementioned challenges are especially significant in cloud settings due to the distribution of data across locations and affiliations. The main issue associated with the centralized model training is the question of data privacy since several parties have to send their data to one universal place. This not only enhances the likelihood of data leakage but also violates rules of data privacy legislation including GDPR and CCPA that regulate the process of transferring or sharing of personal data. Moreover, the growing number and the variety of data sources such as IoT devices, mobile applications, and enterprise systems to name but a few increase challenges with respect to data transfer and processing centrally.

LITERATURE REVIEW

Distributed AI Model Training

According to Shanmugam et al. 2023; Distributed AI model training is a process in which many learning models are trained in parallel using different devices, either owned by different organizations or located at different sites. Several advantages can be outlined: the improvement in the model's scalability, the reduction in the training's length, and the integration of various data sources, which in turn results in greater verisimilitude of the model. Nevertheless, more classical architectures of distributed training, which specify data centralization and transfer learning, have fundamental issues. Data centralization involves the collection of data found in some of the sources to a single point where the model will be trained (Xu et al. 2019).

This has implications that bother the aspect of data privacy since information will be moved from one location to another many times over thus exposing a lot of data to the risk of hacking and other regulatory violations. Thirdly, data centralization may not be feasible for the organizations that have strong restrictions on data localization and storage or when the amounts of generated data are growing significantly.

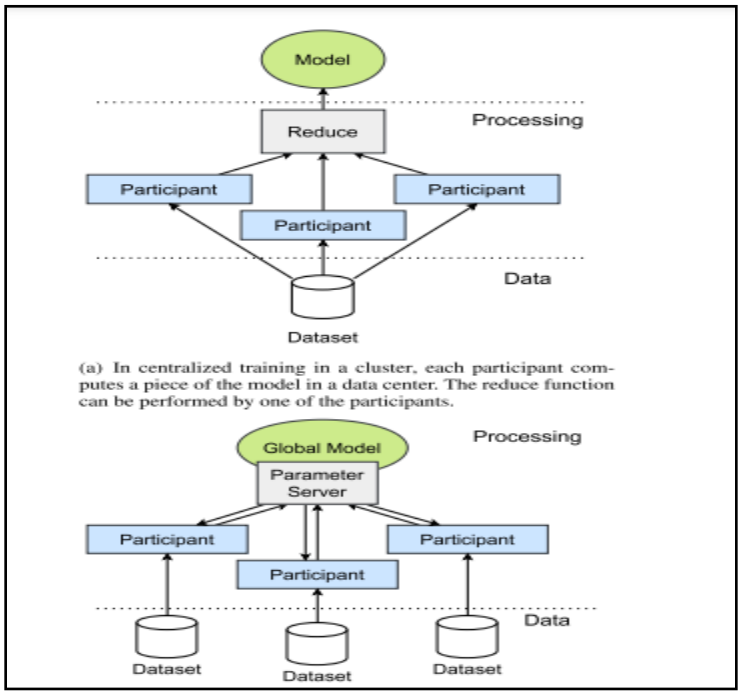


(Source: https://i0.wp.com/neptune.ai/wp-content/uploads/2022/1)

Figure 1: Distributed training

Federated Learning

According to Neto et al. 2023; A recent approach in realizing distributed training of the AI model is federated learning, which provides an improvement over the centralized mode of learning. It allows for the distributed model training without the data consolidation which helps in maintaining the data privacy and respecting data sovereignty. The training is co-ordinated by a central server that sends out a global model to client nodes and takes back their intermediate results for example devices, organizations, or different cloud environments. These clients then feed the model locally with their data and then send only the changes (e. g. , delta weights) back to the central server which in turn updates and enhances the unified model (Yang et al. 2019). Through this method, federated learning eliminates the transfer of the entire dataset or even having access to it and only sends updates of the model, making it secure and compliant with data protection laws. Also, federated learning takes advantage of the sum total of the computing capacity and the available data in the various clients; this results in model learning that is more accurate than what would be achieved through centralized learning.

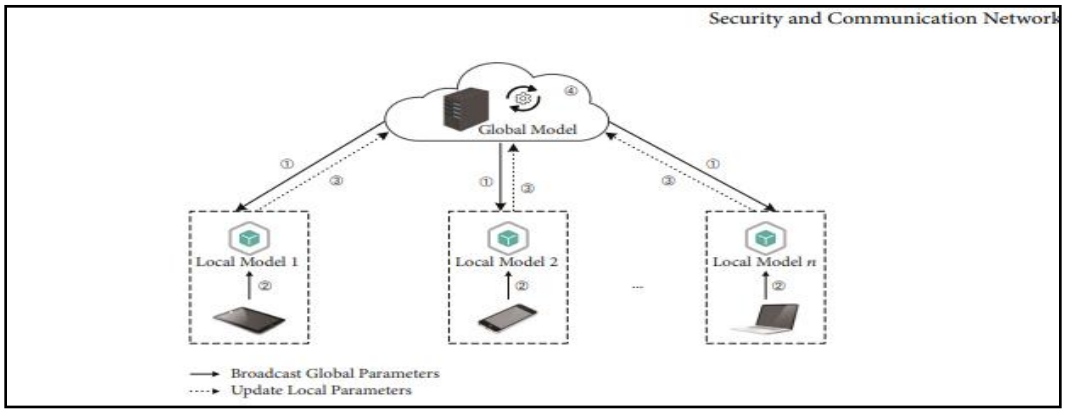


(Source: https://d1wqtxts1xzle7.cloudfront.net/102333266/10107622-libre.pdf)

Figure 1: Different kinds of training

Security and Privacy Considerations

According to Zhang et al. 2022; Although federated learning solves some data privacy issues by keeping the data decentralized, new threats to security and privacy appear here. One of the concerns is that the model's updates or intermediate states containing information about data of the individual clients may leak out, which will give rise to privacy violation or reconstruction attacks. Further, the federated learning system is prone to some security threats and attacks like poisoning attacks, in which the malicious clients try to deceive the global model by providing wrong or adversarial updates. Byzantine failures can also be observed when some clients misbehave and start deviating from the agreed-upon protocol thus threatening the federated learning process's integrity and convergence (Ilias and Georgios 2019). It is therefore imperative that such security and privacy issues are addressed to encourage the trust needed and wider adoption of federated learning, especially in domains involving sensitive data or those operating under strict compliance standards. There are legal requirements in the format of the GDPR and the CCPA regarding data privacy and protection which are the standards to be followed in the architecture and management of federated learning.



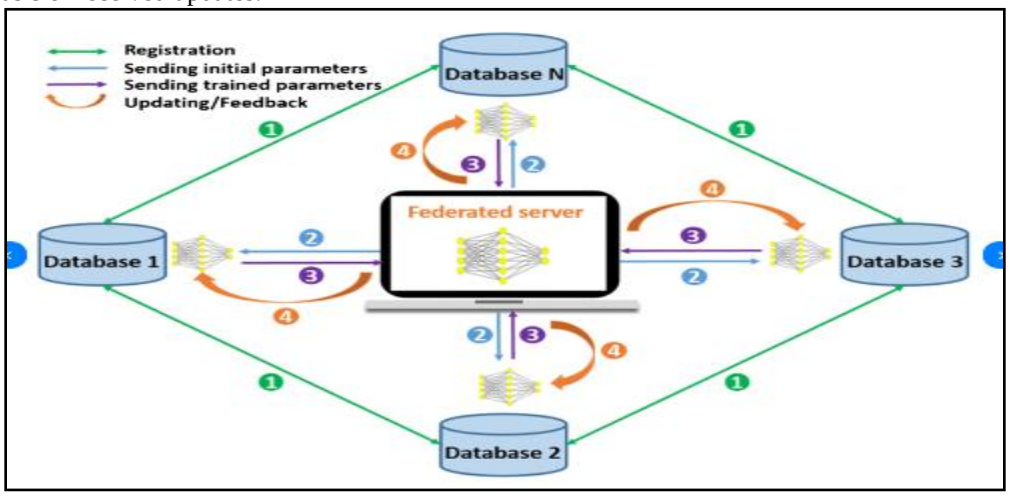
(Source: https://onlinelibrary.wiley.com/doi/pdf/10.1155/2022/2886795)

Figure 3: FL training process

PROPOSED SECURE FEDERATED LEARNING FRAMEWORK

Federated Model Training Pipeline

The federated model training pipeline defines the sequence of activities in the training process across clients (e. g., cloud or organization or devices). In this setup, the central server first sends the copy of the global model to all the clients that will participate in training. Every client re-trains the model on its data using the computational capacity of the corresponding client (Wang et al. 2019). Finally, the clients transmit their updated models to the central server to enhance the global model on the basis of received updates.



(Source: https://www.researchgate.net/publication/349967526/)

Figure 4: Training pipeline

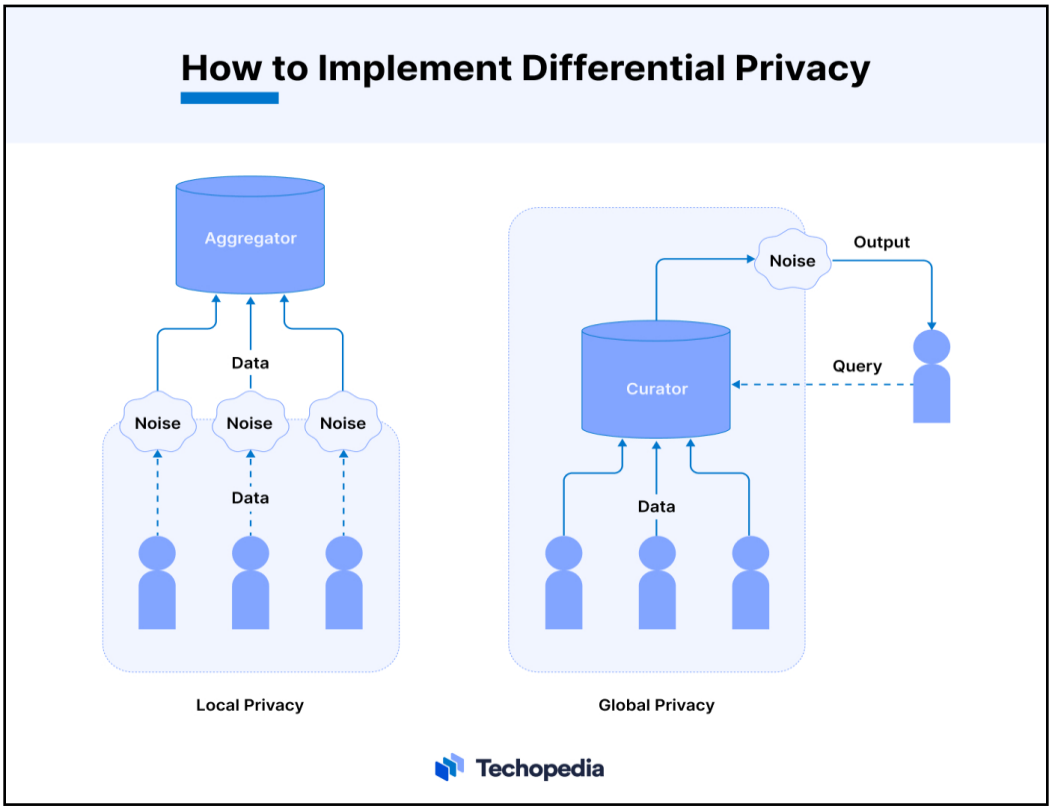
Secure Aggregation and Model Updates

In an attempt to declare the privateness risks, the example also incorporates fix collecting procedures regarding the model updates. These protocols make client updates anonymous. So that the update of one guest cannot be linked to another client's update as well as thus, maintaining the privateness of the clients (Yang et al. 2019). Data collecting techniques like multi-party computation, homomorphic encryption, and derived privateness methods were employed to check that the ferment of aggregating data for the rounded model is fixed and that the ending model's type is preserved.

Differential Privacy and Data Protection

Differential privacy is a proficiency that allows one to protect privateness while analyzing the data in an utile manner. The addressed example also uses derived privateness techniques with the aim of protecting privateness of the clients' data during federated learning.

These mechanisms add a settled sum or 'noise' to the update updates, so that the rounded model could not leak or infer data of the individual clients or their data.



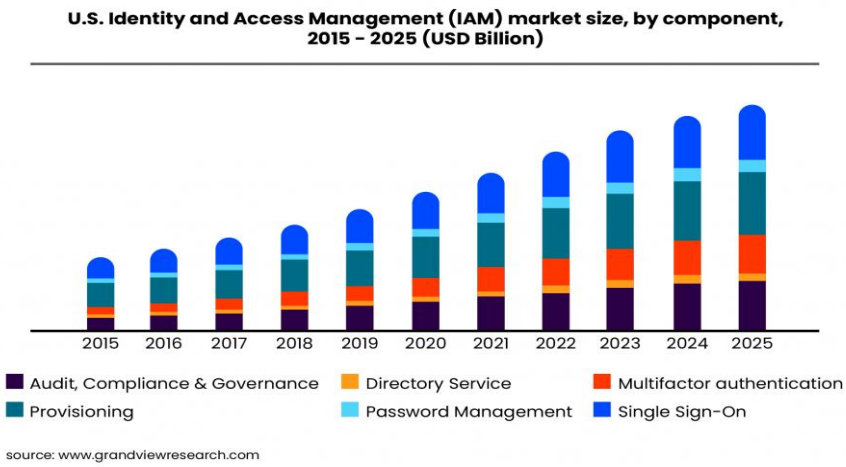
(Source: https://www.techopedia.com/wp-content/uploads/2024)

Figure 5: Different privacy implementation

Identity and Access Management

The federated learning framework of training a model finished data sharing and local update inside a network that was defined by an unquestionable identity and approach direction transcription was built on the principles of credentials as described. The Framework had adopted federated identity direction solutions amplifying guest certification and control when involved in the federated learning process (Preuveneers et al. 2018).

Authentication mechanisms or policies were used in the federated learning entanglement scenario to limit booking only to approved clients for consolidation into the rounded model training.



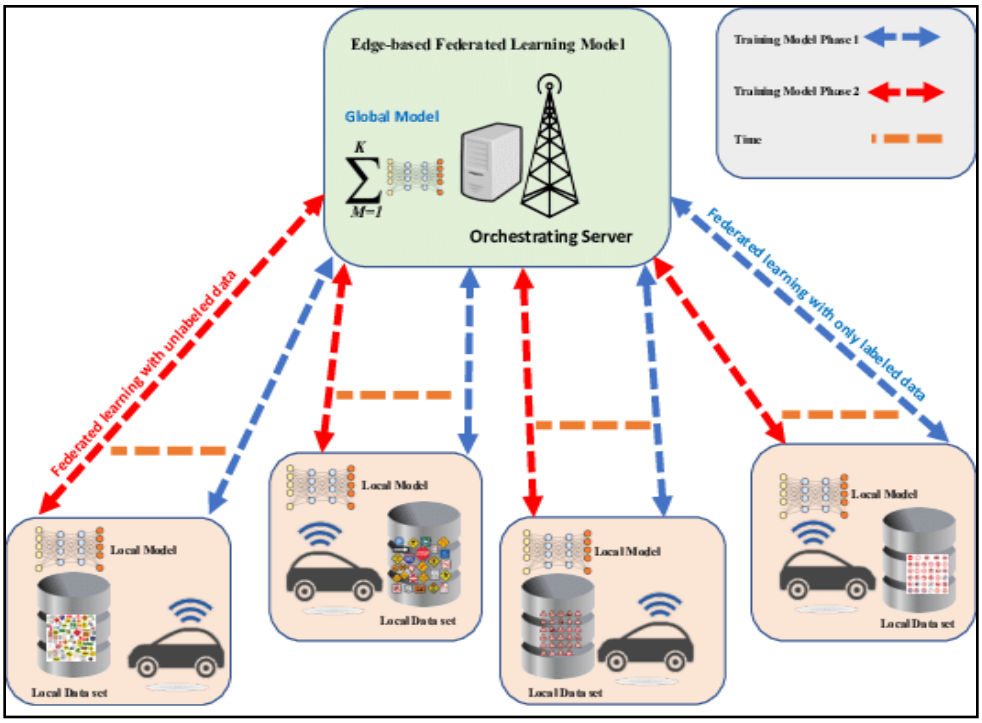
(Source: https://lh6.googleusercontent.com/O2H7185Nsb2nBo6d5FaOzkj)

Figure 6: Access management

METHODS

Federated Learning Setup and Configurations

The federated learning setup can be accomplished by assigning the exchange host and participating clients with appropriate training objectives and modeling the environs of the intended deployment. The method used in this case entails using a central server which is charged with the responsibility of uploading the global model, as well as downloading the models with updates from the numerous clients participating in the procedure (Luo et al. 2019). It also allows clients to train their model on their local data using certain selected machine learning frameworks and hardware aspects like GPU or TPU.

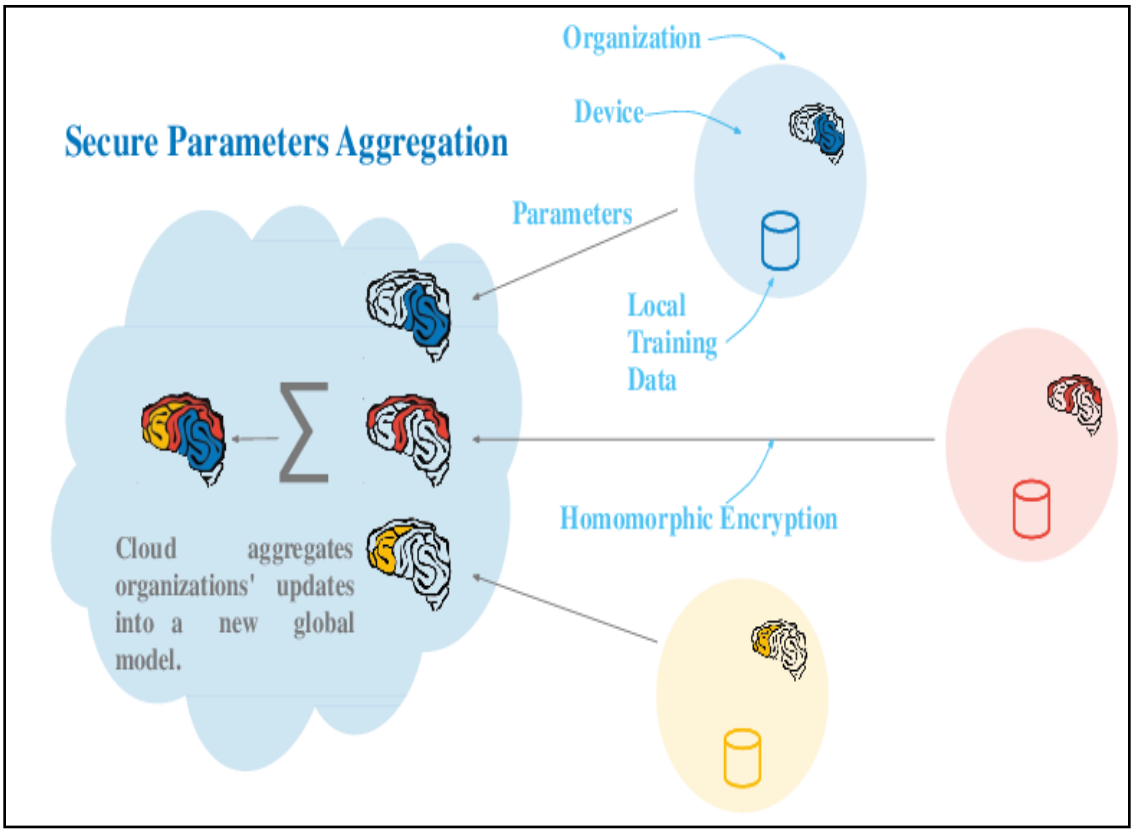


(Source: https://www.researchgate.net/publication/343247609/figure)

Figure 7: Federated Learning Setting

Secure Aggregation Protocols

The instance updates are protected finished fix collecting protocols that also ensured the namelessness of the guest data fed into the federated learning solution. Secure multi party reckoning or SMPC is a result where the exchange host is able to cod updated models from the clients without being able to see the updates of individual shared clients or the data associated with the updates.



(Source: https://www.researchgate.net/profile/Yi-Liu-99/publication/339799244)

Figure 8: Secure and aggregation mechanism

Differential Privacy Mechanisms

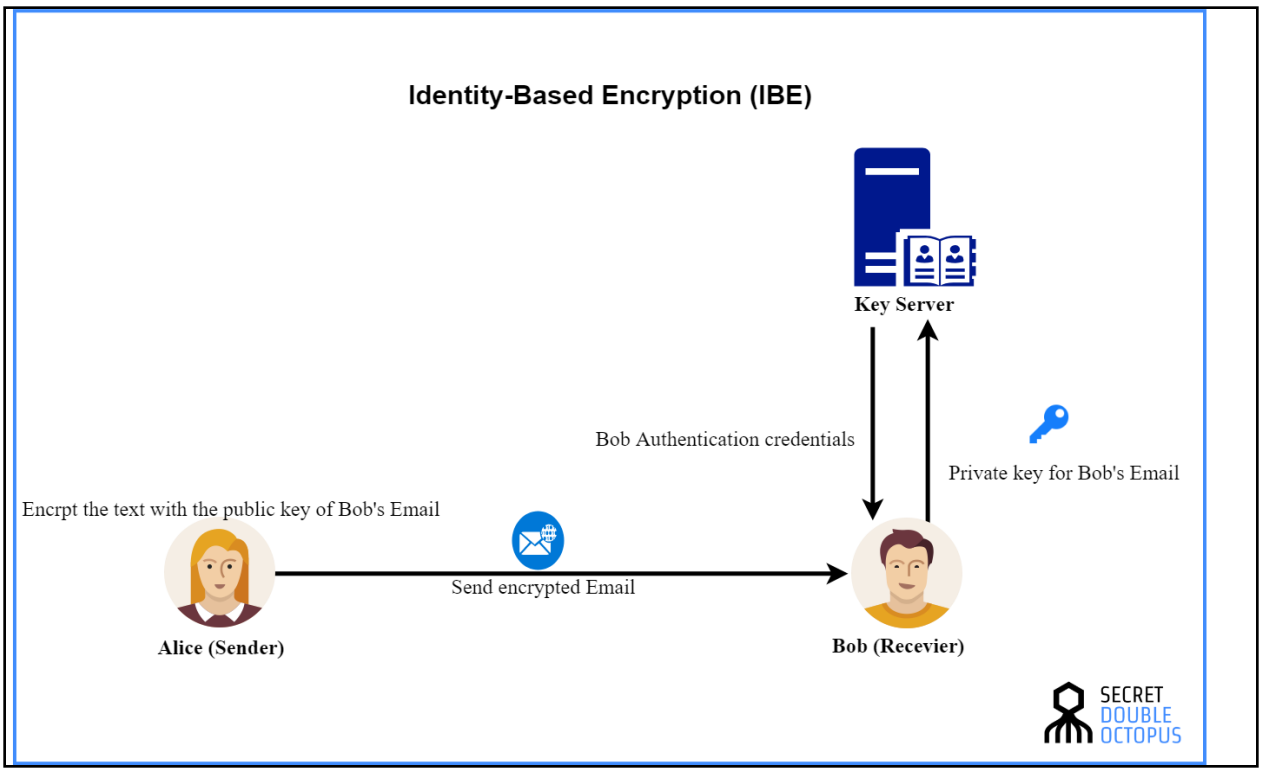
Both adding calibrated noise and perturbing the updates by adding some noise means that the rounded model cannot be used for utilizing or recovering sure data about the appropriate clients or their data (Niu et al. 2019).

Besides, such methods as the Gaussian mechanics that add Freedman noise to the model updates and the exponential mechanics that introduces the randomized reaction methods.

Identity Management and Encryption

The identity and approach direction should be built powerfully to protect the federated learning framework. OAuth2 or Open Connect dissuasive for the federated indistinguishability direction services help to allow clients that take part in the federated learning ferment with the demand certification and authorization (Nishio and Yonetani 2019).

An approach check insurance and mechanics such as the role based approach check RBAC or the attribute based approach check ABAC enable only authorized clients to record in the federated learning entanglement and contributed to the rounded model training.

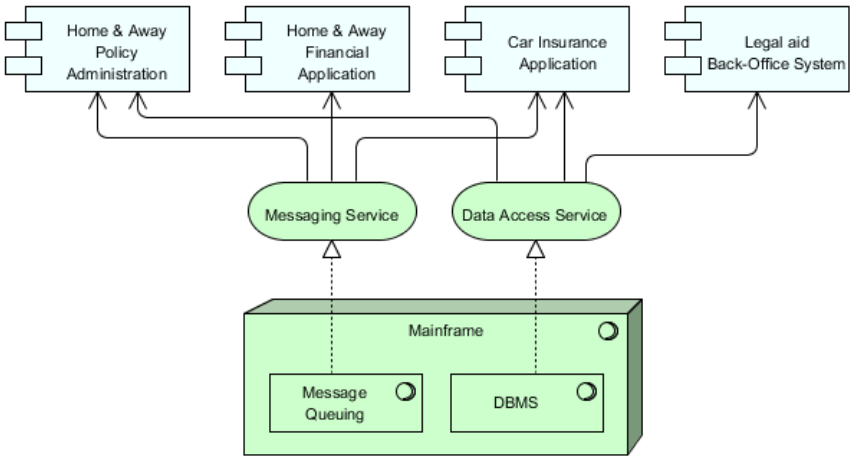


(Source: https://doubleoctopus.com/wp-content/uploads/2021/08/Identity-Based-Encryption.png)

Figure 9: Identity Based Encryption

Implementation and Deployment

There are single authorized factors pertaining to the residue between executing and deployment of the fixed federated learning framework. A iron cloud concentrate transcription was needed in the form of an exchange cloud hub or choline for coordination of the entanglement and the other process resources in client side model solutions (Wang et al. 2019). The given specification can be performed with multiple machine learning libraries and frameworks that support and offer ready-to-use tools for federated learning and secure computation, including TensorFlow Federated, PySyft, or FATE. The incompleteness of data and moving it in and out requires that sufficient attention is given to data integration and these have to be done in a way that merges well with other cloud environments and data sources.



(Source: https://images.visual-paradigm.com/docs/vp_user_guide/11/4455/4456/4458/c_1_6)

Figure 10: Deployment chart

RESULTS

Potential Benefits

The use of a secure federated learning architecture has many potentially desirable features. It helps the organization to utilize distributed data assets and computational power to train accurate and statistically valid AI models while operating within data-protection and legal-restriction constraints (Li et al. 2019). This approach of just passing model updates and keeping data local reduces the chance of data leaks and privacy invasions which are prevalent in the centralized training.

Use Cases and Examples

The idea of secure federated learning has its relevance in several contexts where the data is sensitive or the setting is restrictive in terms of data processing. In healthcare, it may help in joint learning of models for diagnostics or compounds discovery while ensuring patients' data confidentiality. Organizations, especially the financial institutions can use the framework for fraud identification or risk analysis without putting to use the financial data. Federated learning can be used in smart city applications for training models in traffic flow or energy usage while adhering to data ownership.

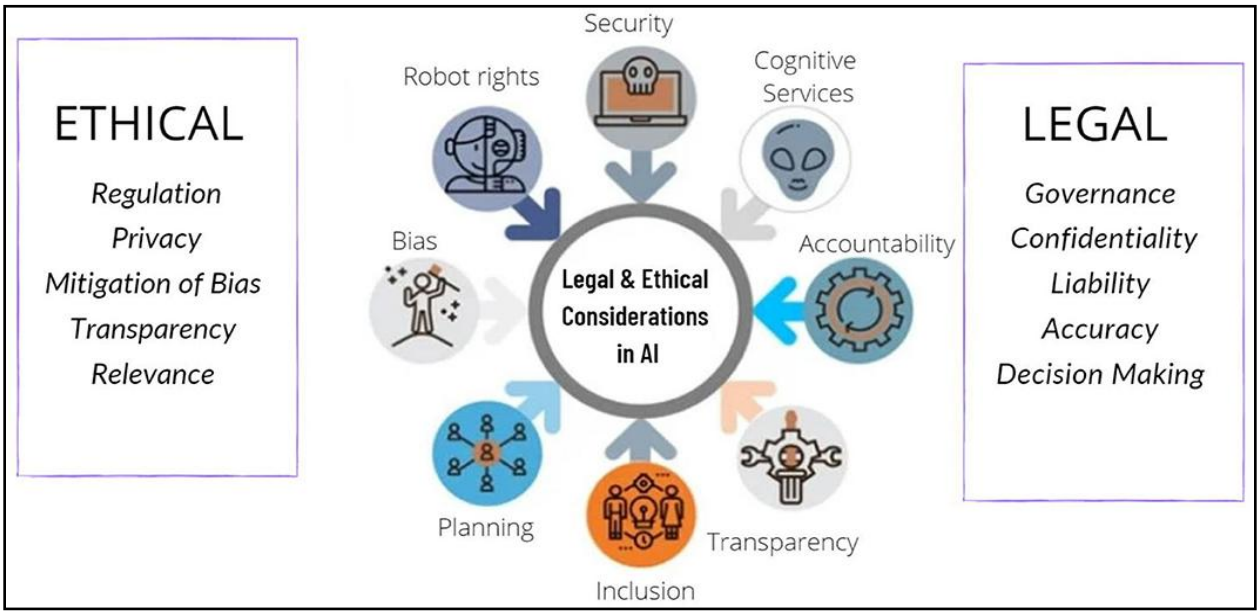
DISCUSSION

Challenges and Limitations

Despite all the benefits of the presented framework, there are several issues and weaknesses that have to be highlighted. There are few issues related to the secure and reliable update and transfer of models within distributed systems especially when the bandwidth or latency is low (Liu et al. 2019). These disadvantages include, namely, scalability since it gets challenging to handle numerous clients or the model architecture increases, affecting the convergence of the FL.

Ethical and Regulatory Considerations

The applications and adoption of secure federated learning solutions need to be steered by an ethical and legal perspective. Some of these are transparency in the model training, accountability, and fairness in the model formation, and proper use of the AI systems. Some specific features of the processing of personal data are adherence to the data protection regulations, including the GDPR and CCPA, focus on minimizing the amount of data collected and stored, limiting its use to the purposes for which it was obtained, and granting data subjects' control over their data.



(Source: https://www.frontiersin.org/files/Articles/862322/fsurg)

Figure 11: Ethical and legal considerations

Future Directions

The improvement in the efficiency of the communication, scalability of the developed approaches, and the enhancement of its robustness should be the future directions in the field of secure federated learning. Research into new compression methods, new layers of architecture, and optimization of the resources used can improve the framework's scalability and the complexity of the models it is capable of training.

CONCLUSION

The proposed secure federated learning framework offers a good solution to federated learning especially with regards to cloud based AI model training while at the same time considering security and privacy risks. Through using secure aggregation protocol, differential privacy and proper identity and access management, the framework reduces the possibility of data breaches, infringement of privacy and malicious attacks. Hence, the major promises for the framework are the enhanced model accuracy and compliance defined under the new regulation, as well as data sovereignty, would be of particular interest to different domains dealing with sensitive data.

REFERENCE LIST

JOURNALS

[1]. Ilias, C. and Georgios, S., 2019, February. Machine learning for all: A more robust federated learning framework. In Proc. 5th Int. Conf. Inf. Syst. Secur. Privacy (pp. 544-551).
[2]. Li, L., Xiong, H., Guo, Z., Wang, J. and Xu, C.Z., 2019, December. SmartPC: Hierarchical pace control in real-time federated learning system. In 2019 IEEE Real-Time Systems Symposium (RTSS) (pp. 406-418). IEEE.
[3]. Sravan Kumar Pala. (2016). Credit Risk Modeling with Big Data Analytics: Regulatory Compliance and Data Analytics in Credit Risk Modeling. (2016). International Journal of Transcontinental Discoveries, ISSN: 3006-628X, 3(1), 33-39.
[4]. Liu, B., Wang, L., Liu, M. and Xu, C.Z., 2019. Federated imitation learning: A privacy considered imitation learning framework for cloud robotic systems with heterogeneous sensor data. arXiv preprint arXiv:1909.00895.
[5]. Luo, J., Wu, X., Luo, Y., Huang, A., Huang, Y., Liu, Y. and Yang, Q., 2019. Real-world image datasets for federated learning. arXiv preprint arXiv:1910.11089.
[6]. Nishio, T. and Yonetani, R., 2019, May. Client selection for federated learning with heterogeneous resources in mobile edge. In ICC 2019-2019 IEEE international conference on communications (ICC) (pp. 1-7). IEEE.
[7]. Niu, C., Wu, F., Tang, S., Hua, L., Jia, R., Lv, C., Wu, Z. and Chen, G., 2019. Secure federated submodel learning. arXiv preprint arXiv:1911.02254.
[8]. Sravan Kumar Pala, "Synthesis, characterization and wound healing imitation of Fe3O4 magnetic nanoparticle grafted by natural products", Texas A&M University - Kingsville ProQuest Dissertations Publishing, 2014. 1572860. Available online at: https://www.proquest.com/openview/636d984c6e4a07d16be2960caa1f30c2/1?pq-origsite=gscholar&cbl=18750
[9]. Preuveneers, D., Rimmer, V., Tsingenopoulos, I., Spooren, J., Joosen, W. and Ilie-Zudor, E., 2018. Chained anomaly detection models for federated learning: An intrusion detection case study. Applied Sciences, 8(12), p.2663.
[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]. Wang, X., Han, Y., Wang, C., Zhao, Q., Chen, X. and Chen, M., 2019. In-edge ai: Intelligentizing mobile edge computing, caching and communication by federated learning. Ieee Network, 33(5), pp.156-165.
[12]. Xu, G., Li, H., Liu, S., Yang, K. and Lin, X., 2019. VerifyNet: Secure and verifiable federated learning. IEEE Transactions on Information Forensics and Security, 15, pp.911-926.
[13]. Jatin Vaghela, A Comparative Study of NoSQL Database Performance in Big Data Analytics. (2017). International Journal of Open Publication and Exploration, ISSN: 3006-2853, 5(2), 40-45. https://ijope.com/index.php/home/article/view/110
[14]. Yang, K., Fan, T., Chen, T., Shi, Y. and Yang, Q., 2019. A quasi-newton method based vertical federated learning framework for logistic regression. arXiv preprint arXiv:1912.00513.
[15]. Yang, Q., Liu, Y., Chen, T. and Tong, Y., 2019. Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology (TIST), 10(2), pp.1-19.