International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Federated Learning in Cybersecurity: Applications, Challenges, and Future Directions

Yamini Kannan

New York, United States
Email: *yk2504[at]nyu.edu*

Abstract: ***Federated learning is an innovative decentralized machine learning technique that offers significant potential for enhancing cybersecurity. By enabling multiple entities to collaboratively train models without sharing raw data, federated learning preserves data privacy and security while leveraging the collective intelligence of diverse datasets. This paper explores the core principles of federated learning, its applications in threat detection, intrusion detection systems (IDS), and malware detection. It also addresses the technical challenges related to data privacy, communication overhead, and model accuracy, providing solutions to overcome these hurdles. Furthermore, the paper discusses future trends and research opportunities, including the integration of federated learning with emerging technologies like blockchain. Through case studies and real-world examples, we demonstrate the effectiveness of federated learning in improving cybersecurity measures. The paper concludes by emphasizing the importance of ongoing research and collaboration to fully realize the potential of federated learning in safeguarding digital infrastructures.***

Keywords: Federated Learning, Cybersecurity, Threat Detection, Intrusion Detection Systems, Malware Detection, Data Privacy, Secure Aggregation, Communication Overhead, Model Accuracy, Blockchain Integration

1. Introduction

In the era of digital transformation, cybersecurity has emerged as a critical concern for organizations across all sectors. With the exponential growth of data and the increasing complexity of cyber threats, traditional security measures are often inadequate in providing robust protection. The need for advanced, adaptive, and privacy-preserving security solutions has never been more pressing. One promising approach that addresses these challenges is federated learning.

Federated learning is an innovative decentralized machine learning technique that enables multiple entities to collaboratively train a model without sharing their raw data. This approach not only enhances data privacy and security but also leverages the computational power of distributed systems. By bringing the model to the data rather than the data to the model, federated learning ensures that sensitive information remains localized while still benefiting from collaborative learning.

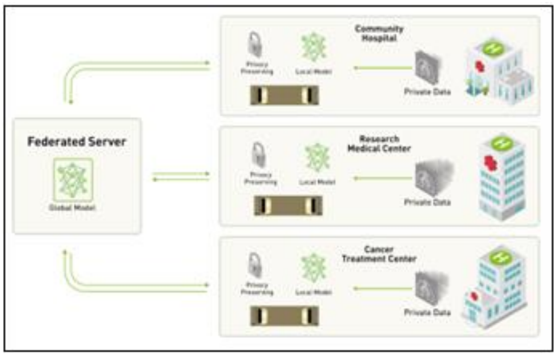
The application of federated learning in cybersecurity offers numerous advantages, including improved threat detection, enhanced privacy, and compliance with data protection regulations. This paper aims to explore the principles and implementation of federated learning in cybersecurity, analyze its impact on threat detection and mitigation, and discuss the challenges and future directions in this burgeoning field.

We will begin by providing an overview of federated learning, highlighting its core principles and components. Next, we will delve into specific applications of federated learning in cybersecurity, such as threat detection, intrusion detection systems (IDS), and malware analysis. We will then examine the technical challenges and solutions associated with federated learning, followed by real-world case studies that demonstrate its effectiveness. Finally, we will explore future trends and research directions that promise to further enhance the capabilities of federated learning in cybersecurity.

2. Overview of Federated Learning

Federated learning is a decentralized approach to machine learning that allows multiple participants to collaboratively train a model without sharing their raw data. Instead of centralizing data in a single location, federated learning distributes the training process across multiple devices or servers, each holding its own local dataset. The core idea is to bring the model to the data rather than bringing the data to the model. After local training, only the model updates (gradients) are shared with a central server, which aggregates these updates to improve the global model. This process is iterated multiple times until the model converges.

Federated learning was first popularized by Google for applications like keyboard prediction, where privacy is paramount, and data is highly sensitive [1]. By enabling collaborative learning without compromising individual data privacy, federated learning has opened new avenues for secure and efficient machine learning.



Federated Learning [10]

3. Core Principles and Components

- Decentralized Data Storage: Data remains on local devices or servers, ensuring that sensitive information is not exposed to potential breaches or misuse. This

Paper ID: MR24706174710 DOI: https://dx.doi.org/10.21275/MR24706174710

decentralization enhances privacy and security by reducing the attack surface.

- Local Model Training: Each participant, or node, trains the model locally on their own dataset. This local training leverages the computational power of edge devices, such as smartphones, IoT devices, or local servers.
- Model Update Aggregation: After local training, nodes share model updates (e.g., gradients or weights) with a central server. The central server aggregates these updates using techniques like Federated Averaging (FedAvg) [2], which combines the updates to improve the global model.
- Iterative Process: The federated learning process is iterative, with multiple rounds of local training and global aggregation. This iterative approach ensures that the global model continuously improves while preserving data privacy.
- Secure Communication: To protect the integrity and confidentiality of model updates, federated learning employs secure communication protocols. Techniques like Secure Multiparty Computation (SMC) and Homomorphic Encryption are used to ensure that updates are securely transmitted and aggregated [3].

Key Tenets of Zero Trust:

- Never Trust, Always Verify: This foundational principle emphasizes that no entity—whether inside or outside the network—should be trusted by default. Every access request must be authenticated and authorized before granting access. This continuous verification process ensures that trust is established dynamically and contextually, based on the current state of the user, device, and network.
- Least Privilege Access: Zero Trust advocates for granting the minimal level of access necessary for users and devices to perform their tasks. This principle reduces the potential impact of a security breach by limiting the lateral movement of attackers within the network. Access policies are granular and continually evaluated to ensure compliance with this principle.
- Micro-Segmentation: Traditional networks often rely on broad segmentation, creating large trust zones that can be exploited by malicious actors. Zero Trust employs micro-segmentation to divide the network into smaller, isolated segments. Each segment is protected with its own security controls, and communication between segments is tightly controlled and monitored.
- Continuous Monitoring and Analytics: Zero Trust requires constant monitoring and analysis of network traffic, user behavior, and system activities. Advanced analytics and machine learning techniques are used to detect anomalies and potential threats in real-time. This continuous assessment allows for rapid detection and response to security incidents.
- Identity and Access Management (IAM): Identity is at the core of Zero Trust. Robust IAM solutions are employed to ensure that users and devices are accurately identified and authenticated. Multi-factor authentication (MFA), single sign-on (SSO), and adaptive authentication methods are used to enhance security and user experience.

1) *Comparison with Traditional Security Models*

Differences Between Perimeter-Based Security and Zero Trust:

a) Trust Assumptions:

- Traditional Security: Assumes that users and devices inside the network perimeter are trustworthy, while those outside are not. Security measures focus on protecting the boundary, creating a strong perimeter defense.
- Zero Trust: Assumes that no user or device should be trusted by default, regardless of their location. Trust is established dynamically through continuous verification and context-aware policies.

b) Access Control:

- Traditional Security: Utilizes broad access controls that grant extensive permissions once inside the network. This can lead to excessive privileges and increased risk of lateral movement by attackers.
- Zero Trust: Implements granular access controls based on the principle of least privilege. Access is granted on a need-to-know basis, minimizing the potential impact of security breaches.

c) Network Segmentation:

- Traditional Security: Often relies on coarse segmentation, creating large trust zones that can be exploited by attackers once they gain access.
- Zero Trust: Employs micro-segmentation to create smaller, isolated segments. Each segment has its own security controls, reducing the risk of lateral movement and containing potential threats.

d) Monitoring and Detection

- Traditional Security: Relies on periodic monitoring and signature-based detection methods, which can be slow to respond to new and evolving threats.
- Zero Trust: Utilizes continuous monitoring and advanced analytics to detect anomalies and potential threats in real-time. Machine learning and behavioral analysis enhance the accuracy and speed of threat detection.

2) *Advantages of Zero Trust Over Traditional Models:*

a) Enhanced Security:

Zero Trust provides a more robust security framework by continuously verifying trust and implementing least privilege access. This reduces the likelihood of breaches and limits the impact of successful attacks.

b) Adaptability:

Zero Trust is well-suited to modern IT environments, including cloud computing, remote work, and mobile devices. It provides a flexible and scalable security model that can adapt to changing threats and technologies.

c) Reduced Attack Surface

By implementing micro-segmentation and granular access controls, Zero Trust significantly reduces the attack surface. This makes it more difficult for attackers to move laterally within the network and compromise additional resources.

d) Improved Compliance:

Zero Trust facilitates compliance with regulatory requirements by enforcing strict access controls and continuous monitoring. Detailed audit logs and real-time analytics provide visibility into user activities and system events.

e) User-Centric Security:
Zero Trust focuses on securing individual users and devices, rather than relying solely on network boundaries. This user-centric approach enhances security in dynamic and distributed environments, where traditional perimeter defenses are less effective.

3) Comparison with Traditional Machine Learning

a) Data Centralization:

- Traditional Machine Learning: Centralizes data in a single repository, requiring all participants to share their raw data. This centralization poses significant privacy and security risks, as well as challenges related to data governance and compliance.
- Federated Learning: Distributes the training process across multiple nodes, keeping data decentralized and localized. Only model updates are shared, significantly mitigating privacy and security concerns [4].

b) Scalability:

- Traditional Machine Learning: Scalability is often limited by the central server's capacity to handle large volumes of data and computational load.
- Federated Learning: Leverages the computational power of edge devices and local servers, enabling scalable training across a vast number of participants. This distributed approach reduces the central server's burden and enhances overall system scalability [5].

c) Latency and Bandwidth:

- Traditional Machine Learning: Requires substantial bandwidth and low latency for transferring large datasets to the central server.
- Federated Learning: Reduces bandwidth requirements by only transmitting model updates, which are typically much smaller than raw data. This efficiency makes federated learning suitable for environments with limited bandwidth and higher latency [6].

4) Advantages of Federated Learning in Terms of Privacy and Data Security:

- Enhanced Privacy: By keeping data on local devices, federated learning ensures that sensitive information is never exposed to potential breaches or misuse. This privacy-preserving approach is particularly valuable in domains like healthcare, finance, and personal devices, where data sensitivity is paramount [7].
- Compliance with Regulations: Federated learning aligns with data protection regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). By decentralizing data storage and processing, organizations can more easily comply with stringent data privacy requirements [8].
- Robustness Against Attacks: Decentralizing data storage reduces the risk of single points of failure and makes it more challenging for attackers to compromise the entire dataset. Techniques like differential privacy and secure aggregation further enhance the security of model updates, making federated learning a robust solution against adversarial attacks [9].

4. Applications of Federated Learning in Cybersecurity

a) Threat Detection and Intelligence Sharing

Federated learning significantly enhances threat detection by enabling collaborative learning across multiple organizations or devices without the need to share sensitive data. In traditional threat detection systems, data centralization can pose significant privacy and security risks, as well as logistical challenges. Federated learning addresses these issues by allowing each participant to train a local model on their own data and then share only the model updates (such as gradients) with a central server. This server aggregates the updates to create a global model that benefits from the collective knowledge of all participants.

By leveraging federated learning, organizations can detect threats more accurately and quickly. The aggregated model can identify patterns and anomalies that might not be evident in a single dataset but become apparent when multiple datasets are combined. This collaborative approach allows for a more comprehensive and robust threat detection system, as the diversity of data sources enhances the model's ability to generalize and detect a wider range of threats.

b) Examples of Collaborative Threat Intelligence Sharing Among Organizations:

- Financial Sector: Financial institutions often face similar types of cyber threats, such as fraud and phishing attacks. By using federated learning, banks and financial organizations can collaborate to improve their threat detection capabilities. Each institution trains a local model on its own transaction data, identifying fraudulent patterns. The model updates are then shared and aggregated, resulting in a global model that can detect new and emerging fraud patterns more effectively.
- Healthcare Sector: In the healthcare industry, protecting patient data is paramount, yet there is a need to collaborate on detecting cybersecurity threats such as ransomware and data breaches. Federated learning enables hospitals and healthcare providers to train models on their local data while sharing insights through model updates. This approach allows for enhanced threat detection without compromising patient privacy.
- Telecommunications: Telecommunications companies can use federated learning to detect and mitigate Distributed Denial of Service (DDoS) attacks and other network-based threats. By collaborating on threat intelligence, telecom providers can create a more resilient and adaptive detection system, leveraging the diverse data from different network environments.

c) Intrusion Detection Systems (IDS)

Intrusion Detection Systems (IDS) are critical for monitoring network traffic and identifying potential security breaches. Traditional IDS often rely on centralized data collection and analysis, which can be limited by the availability and diversity of data. Federated learning offers a novel approach to enhance

IDS by enabling decentralized training across multiple network nodes or organizations.

In a federated learning-based IDS, each node trains a local model on its own network traffic data, identifying patterns indicative of potential intrusions. The model updates are then shared with a central server, which aggregates them to create a global IDS model. This global model benefits from the diverse data sources, improving its ability to detect a wide range of intrusions.

d) Case Studies and Real-World Implementations:

- Corporate Networks: Large corporations with multiple branch offices can use federated learning to enhance their IDS. Each branch office trains a local IDS model on its own network traffic, identifying suspicious patterns. The model updates are aggregated to create a global IDS model that can detect intrusions across the entire corporate network. This approach not only improves detection accuracy but also enhances the system's resilience against targeted attacks on individual branches.
- Cloud Service Providers: Cloud service providers can implement federated learning to improve their IDS capabilities across different data centers and client environments. Each data center or client trains a local IDS model on its specific network traffic, contributing to a global model that benefits from the diverse and distributed nature of cloud environments. This collaborative approach enables more effective detection of sophisticated attacks that may target multiple clients or data centers simultaneously.
- Smart Grids: In smart grid environments, federated learning can be used to enhance IDS for monitoring critical infrastructure. Each component of the smart grid, such as substations and control centers, trains a local IDS model on its operational data. The aggregated global model can detect anomalies and potential intrusions across the entire grid, ensuring the security and reliability of the energy supply.

e) Malware Detection and Analysis

Malware detection and analysis are crucial for protecting systems and networks from malicious software. Traditional malware detection methods often rely on centralized databases of known malware signatures, which can be slow to update and limited in their ability to detect new and evolving threats. Federated learning provides a decentralized approach that enhances malware detection by leveraging collaborative learning across multiple devices and organizations.

In a federated learning-based malware detection system, each participant trains a local model on its own data, identifying features and patterns associated with malware. The model updates are then shared with a central server, which aggregates them to create a global malware detection model. This global model benefits from the diverse data sources, improving its ability to detect a wide range of malware, including zero-day threats.

f) Benefits and Challenges in the Context of Malware Detection:

Benefits:

- Improved Detection Accuracy: Federated learning enhances the accuracy of malware detection by combining insights from multiple data sources. The aggregated global model can identify malware patterns that may not be evident in a single dataset, resulting in more robust and comprehensive detection capabilities.
- Privacy Preservation: By keeping data on local devices, federated learning ensures that sensitive information is not exposed to potential breaches or misuse. This privacy-preserving approach is particularly valuable in industries where data sensitivity is paramount, such as healthcare and finance.
- Adaptability: Federated learning enables the rapid adaptation of malware detection models to new and evolving threats. As new malware samples are detected and analyzed locally, the global model can quickly incorporate these insights, ensuring that the detection system remains up-to-date and effective.

Challenges:

- Data Heterogeneity: One of the main challenges in federated learning for malware detection is dealing with heterogeneous data sources. Different devices and organizations may have varying data formats, feature sets, and labeling standards, which can complicate the aggregation and training process.
- Communication Overhead: Federated learning requires frequent communication between local nodes and the central server to share model updates. This communication can introduce overhead and latency, especially in environments with limited bandwidth or high network latency.
- Model Synchronization: Ensuring the consistency and synchronization of models across decentralized nodes is a complex task. Techniques like Federated Averaging (FedAvg) and secure aggregation are used to address these challenges, but they may not fully eliminate the risk of model divergence or conflicts.

5. Technical Challenges and Solutions

5.1 Data Privacy and Security

One of the primary advantages of federated learning is its ability to preserve data privacy by keeping data on local devices. However, ensuring that privacy is maintained throughout the process requires robust techniques to prevent leakage of sensitive information through model updates.

Techniques for Secure Aggregation and Differential Privacy:

- Secure Aggregation: Secure aggregation protocols are designed to ensure that the model updates shared by local nodes are aggregated in a way that prevents the central server from accessing individual updates. Techniques such as Secure Multiparty Computation (SMC) and Homomorphic Encryption allow for the aggregation of encrypted updates, ensuring that only the aggregated result is revealed [1].

- Differential Privacy: Differential privacy adds noise to the model updates before they are shared, making it difficult for adversaries to infer specific information about the local data. This technique ensures that the privacy of individual data points is preserved while still allowing for effective model training [2].

Communication and Computation Overhead

Federated learning requires frequent communication between local nodes and the central server to share model updates. This communication can introduce significant overhead, particularly in environments with limited bandwidth or high network latency. Additionally, the computational load on local devices can be substantial, especially when dealing with large models or datasets.

Solutions Such as Model Compression and Efficient Communication Protocols:

- Model Compression: Techniques such as quantization, pruning, and sparse updates can reduce the size of the model updates, thereby decreasing the amount of data that needs to be transmitted. These compression techniques can significantly reduce communication overhead without substantially impacting model performance [3].
- Efficient Communication Protocols: Protocols like Federated Averaging (FedAvg) reduce the frequency of communication by allowing local nodes to train for multiple iterations before sending updates to the central server. Other techniques, such as asynchronous communication and hierarchical aggregation, can further enhance communication efficiency by structuring the communication process more effectively [4].

Model Accuracy and Consistency

Maintaining model accuracy and consistency in a federated learning environment is challenging due to the decentralized nature of the training process. Variations in local data distributions, network conditions, and computational capabilities can lead to model divergence or inconsistencies.

Techniques for Model Synchronization and Conflict Resolution:

- Federated Averaging (FedAvg): FedAvg is a widely used technique that aggregates model updates from local nodes by averaging them. This approach helps to mitigate the effects of data heterogeneity and ensures that the global model benefits from the collective knowledge of all participants [5].
- Adaptive Learning Rates: Adjusting learning rates based on the performance of local models can help to ensure that updates from nodes with more informative data are weighted more heavily. This adaptive approach can enhance the accuracy and consistency of the global model [6].
- Conflict Resolution: Techniques such as gradient clipping and consensus algorithms can be used to resolve conflicts that arise from divergent model updates. These methods ensure that the global model remains stable and converges effectively despite variations in local training processes [7].

6. Future Trends and Developments

Emerging Trends in Federated Learning

- New Frameworks and Tools: As federated learning continues to gain traction, new frameworks and tools are being developed to facilitate its implementation and enhance its capabilities. Platforms like TensorFlow Federated (TFF) and PySyft are designed to simplify the development and deployment of federated learning models, offering built-in functionalities for secure aggregation, differential privacy, and efficient communication [1]. These frameworks provide developers with the necessary tools to build robust federated learning systems while addressing key challenges such as scalability and security.
- Integration with Other Emergig Technologies: One promising direction for federated learning is its integration with other emerging technologies, such as blockchain. Blockchain's decentralized and immutable nature can enhance the security and transparency of federated learning processes. By using blockchain to securely record and verify model updates, organizations can ensure the integrity and trustworthiness of the federated learning process. Additionally, smart contracts can automate the enforcement of privacy policies and compliance requirements, further enhancing the robustness of the system [2].

Open Research Questions

Despite the advancements in federated learning, several challenges remain unresolved and warrant further research:

- Data Heterogeneity: The variability in data distributions across different nodes can lead to model divergence and reduced performance. Research is needed to develop techniques that can effectively handle data heterogeneity and ensure consistent model performance across diverse datasets [3].
- Efficient Communication: Reducing communication overhead remains a critical challenge in federated learning. Future research should focus on developing more efficient communication protocols and compression techniques that minimize the data transmitted without compromising model accuracy [4].
- Privacy-Preserving Techniques: While differential privacy and secure aggregation are effective, there is a need for more advanced privacy-preserving techniques that can provide stronger guarantees without significantly impacting model performance. Research in homomorphic encryption and secure multi-party computation (SMC) holds promise in this area [5].

Potential Advancements in Federated Learning for Cybersecurity:

- Real-Time Threat Detection: Future advancements in federated learning could enable real-time threat detection and response systems. By leveraging edge computing and real-time data processing, federated learning models can quickly identify and mitigate cyber threats as they occur, enhancing the overall security posture of organizations [6].
- Adaptive Security Models: Adaptive federated learning models that can dynamically adjust to new threats and evolving attack patterns will be crucial for future

cybersecurity applications. These models can continuously learn from new data and adapt their strategies to counter emerging threats effectively [7].

- Collaborative Cybersecurity Networks: The development of collaborative cybersecurity networks, where multiple organizations share threat intelligence and collaboratively train federated learning models, will enhance the collective defense against cyber threats. These networks can leverage the diverse data and expertise of participating organizations to build more robust and comprehensive security systems [8].

In summary, the future of federated learning in cybersecurity holds significant promise, with emerging trends and open research questions paving the way for innovative solutions. By addressing these challenges and exploring new avenues, federated learning can continue to evolve and provide advanced, privacy-preserving security solutions for the digital age.

7. Conclusion

Federated learning represents a transformative approach to addressing the complex and evolving challenges in cybersecurity. By enabling collaborative model training without the need to share raw data, federated learning preserves data privacy and security while leveraging the collective intelligence of multiple entities. This paper has explored the core principles of federated learning, its applications in cybersecurity, the technical challenges it faces, and the solutions to overcome these challenges.

In the realm of threat detection and intelligence sharing, federated learning allows organizations to pool their insights and develop more robust models for identifying and mitigating cyber threats. The use of federated learning in Intrusion Detection Systems (IDS) enhances the ability to detect and respond to intrusions across diverse network environments. Additionally, federated learning's application in malware detection and analysis provides a decentralized approach to identifying and combating malicious software, significantly improving detection accuracy and adaptability.

Despite its advantages, federated learning poses several technical challenges, including ensuring data privacy, managing communication and computation overhead, and maintaining model accuracy and consistency. Techniques such as secure aggregation, differential privacy, model compression, and adaptive learning rates are critical in addressing these challenges and enabling successful implementations of federated learning in cybersecurity.

Looking forward, the future of federated learning in cybersecurity is promising, with emerging trends and new frameworks enhancing its capabilities. The integration of federated learning with technologies like blockchain can further strengthen security and transparency. However, several open research questions remain, particularly in handling data heterogeneity, improving communication efficiency, and developing advanced privacy-preserving techniques. To fully realize the potential of federated learning in cybersecurity, ongoing research and innovation are essential. By addressing the unresolved challenges and exploring new avenues, federated learning can evolve to provide even more advanced, adaptive, and privacy-preserving security solutions. As organizations continue to collaborate and leverage federated learning, the collective defense against cyber threats will be strengthened, ensuring a more secure digital future.

In conclusion, federated learning offers a powerful framework for enhancing cybersecurity in a privacy-preserving manner. Its ability to enable collaborative learning across decentralized data sources makes it a valuable tool in the fight against cyber threats. Continued research, development, and collaboration will be key to unlocking the full potential of federated learning and ensuring its success in safeguarding digital infrastructures.

Acknowledgment

The author would like to extend sincere thanks to New York University for graciously providing the resources to conduct the research.

References

[1] Konecny, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T., & Bacon, D. (2016). "Federated Learning: Strategies for Improving Communication Efficiency." arXiv preprint arXiv:1610.05492.
[2] McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017). "Communication-Efficient Learning of Deep Networks from Decentralized Data." Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS).
[3] Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., ... & Seth, K. (2017). "Practical Secure Aggregation for Privacy-Preserving Machine Learning." Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS).
[4] Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). "Federated Machine Learning: Concept and Applications." ACM Transactions on Intelligent Systems and Technology (TIST), 10(2), 1-19.
[5] Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). "Federated Learning: Challenges, Methods, and Future Directions." IEEE Signal Processing Magazine, 37(3), 50-60.
[6] Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., ... & Zhao, S. (2021). "Advances and Open Problems in Federated Learning." arXiv preprint arXiv:1912.04977.
[7] Shokri, R., & Shmatikov, V. (2015). "Privacy-Preserving Deep Learning." Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS).
[8] European Parliament and Council of the European Union. (2016). "General Data Protection Regulation (GDPR)." Official Journal of the European Union.
[9] Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2016). "Deep Learning with Differential Privacy." Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS).
[10] Nicole R., "What is Federated Lerning". Nvidia BLOG