International Journal of Science and Engineering Applications
Volume 15-Issue 04, 16 – 22, 2026, ISSN:- 2319 - 7560
DOI: 10.7753/IJSEA1504.1003

Federated Learning for Privacy-Preserving Network Security Across Healthcare Providers

Zubair Ahmed Mohammed
Department of Technology Management
Lindsey Wilson College
KY, USA

Syed Saifuddin Ahmed Muzaffar
Department of Information Technology
Campbellsville University, KY, USA

Devasis Pradhan
Assistant Director of Research at Acharya Institutes,
Bengaluru, India

Mukul Shirvaikar
Professor of Electrical and Computer Engineering,
University of Texas at Tyler
USA

***Abstract*—** Hackers are employing increasingly advanced methods to target hospital networks, electronic health data, medical IoT devices, and telemedicine apps as the healthcare industry becomes more digitally integrated. Gathering and sharing private medical information is essential when employing centralized machine learning to identify intrusions. Important concerns are privacy, regulations, and compliance with HIPAA, GDPR, and other laws. Federated Learning (FL) is an approach to learning that protects patient data and does not depend on a central server. It makes it possible for different healthcare facilities to work together to create efficient security models. This study looks at the ways that FL can enhance network security and preserve privacy in the healthcare industry. It explores secure aggregation techniques, federated learning systems, differential privacy strategies, and strong defences against inference and poisoning attacks. By using a hierarchical federated framework, this study shows how multi-provider healthcare organizations can increase detection accuracy while preserving their independence, privacy, and compliance.

***Keywords*—** Data security, safe aggregation, cybersecurity, medical IoT security, distributed artificial intelligence, intrusion detection systems, federated learning, privacy-preserving machine learning, healthcare cybersecurity, and differential privacy All of these examples demonstrate what compliance implies.

I. INTRODUCTION

The healthcare sector is changing quickly as a result of telemedicine platforms, cloud-based hospital management systems, electronic health records, and an increase in medical IoT devices [1]. In addition to simplifying hospital operations and patient care, these technologies increase the susceptibility of healthcare networks to cyberattacks. Ransomware assaults, DDoS attacks, insider threats, and data breaches have increased in frequency in healthcare businesses due to the high value of protected health information (PHI). Machine learning-based intrusion detection systems, which require data from several sources for efficient training, may be used in traditional network security. However, keeping all of your medical records in one location could cause privacy and legal problems.

But laws like GDPR and HIPAA make it illegal for companies to share data, which makes it harder for cybersecurity teams to work together [2]. Since it enables numerous healthcare companies to train a shared security model without sharing any data, federated learning (FL) is a great strategy. Federated Learning only offers encrypted model updates that meet the requirements and safeguard the data of each school. This study investigates how federated learning might assist linked healthcare organizations in enhancing network security while preserving privacy.

International Journal of Science and Engineering Applications
Volume 15-Issue 04, 07 – 15, 2026, ISSN:- 2319 - 7560
DOI: 10.7753/IJSEA1504.1003

II. Fundamentals of Federated Learning

A technique for computer learning called federated learning (FL) enables users to work together across devices or places without needing to save all of the raw data in one spot. H. Brendan McMahan and his colleagues at Google made it possible [3]. Allowing each participant—for example, a hospital or health network—to train a model with their own data and only transmit encrypted changes to the model is the aim. In the healthcare sector, where maintaining patient privacy is essential, this is also helpful.

A. Basic Architecture

The conventional FL configuration is composed of three essential components:

- Client nodes: hospitals, clinics, or healthcare organizations that train models on their own data—private network traffic and healthcare IoT data [4].
- Central aggregation server: manages training rounds and aggregates model updates via secure aggregation.
- Communication layer: ensures that model parameters are sent over the communication layer while encrypted.

Normally, the training process involves iterative rounds where the server broadcasts a global model, and the clients update the global model, resulting in a new global model.

Table 1: Federated Learning Types

FL Type	Description	Healthcare Example
Horizontal FL	Same feature space, different data samples	Multiple hospitals with similar EHR schemas
Vertical FL	Different feature sets, shared patient overlap	Hospital + insurance provider collaboration
Federated Transfer Learning	Minimal overlap in data/features	Cross-country healthcare analytics

B. Optimization Algorithms

The optimization methods used in Federated Learning are:

- Federated Averaging (FedAvg): The client model parameters are averaged to update the global model.
- FedProx: This method is used to handle non-IID data in the healthcare domain [5].
- Secure Aggregation: The updates are aggregated in such a way that the server does not receive the individual updates.
- Differentially Private SGD: Noise is added to the gradients to prevent privacy attacks.

These methods can be used to provide a scalable solution for collaborative intelligence in the healthcare network security system.

III. . Privacy and Security in Healthcare Networks

Healthcare organizations combine technology and humans. They oversee some of the most private digital data. Financial information, insurance, Protected Health Information (PHI), and real-time data from medical equipment are all handled by hospitals, clinics, and telemedicine centers [6]. This makes them a desirable target for cybercrime organizations, ransomware attackers, and even staff members. The impact of an attack extends beyond businesses to include life-saving services. Our healthcare system is extremely susceptible to connectivity issues, as the WannaCry attack showed. It hurt a lot of nations.

Cloud storage, IoT medical devices (such MRI scanners and infusion pumps), EHR servers, and remote access interfaces are examples of healthcare systems [7]. Adding mobile health apps to telemedicine expands the number of access points. Attackers may use outdated legacy systems, exposed endpoints, and weak login systems to commit phishing, malware, DDoS, and data theft.

Privacy laws, such as GDPR and HIPAA, place strict restrictions on how organizations handle and share data. Patient data must be kept confidential, safe, and easily available, but these rules also make it more challenging to compile data for security analytics powered by artificial intelligence [8]. Security and compliance issues may arise when conventional centralized machine learning algorithms are used.

This is addressed via federated learning, which guarantees the security of network and patient data across all institutions [9]. We may thus work together to detect dangers while abiding by all legal requirements and privacy policies.

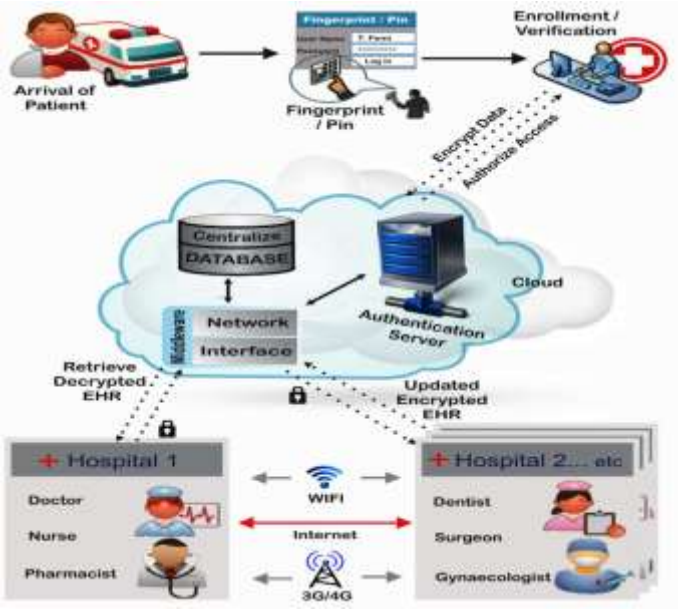

Figure 1: Healthcare Network Threat Surface

IV. Federated Learning for Network Security

Without disclosing patient information or network traffic, Federated Learning (FL) enables healthcare

International Journal of Science and Engineering Applications
Volume 15-Issue 04, 07 – 15, 2026, ISSN:- 2319 - 7560
DOI: 10.7753/IJSEA1504.1003

companies to work together and exchange cybersecurity knowledge [10]. Every healthcare facility creates its own algorithms for detecting intrusions and anomalies rather than keeping all logs or data collection in one place. They only provide the coordinating server with encrypted model changes. This tactic raises everyone's awareness of potential risks while protecting people's privacy.

A. Use Cases in Healthcare Network Security

1. Federated Intrusion Detection Systems (F-IDS): By pooling their IDS model training resources, hospitals can identify ransomware, DDoS assaults, and insider threats in their distributed networks [11].
2. Malware and Ransomware Classification: Local endpoints look for dangerous binaries, and the more data they get from different sources, the more adept they get at spotting them [12].
3. IoT Medical Device Anomaly Detection: Federated learning models keep an eye on unexpected communication between devices like respirators, imaging equipment, and infusion pumps. Ransomware, denial-of-service attacks, or unauthorized shutdown of scanners and gateways may be indicated if the CT-based model shows an abrupt decrease in case volume, modality diversity, or exam time that deviates from clinical schedules.
4. Secure Imaging workflow monitoring: Predicted tumor distributions, acquisition patterns, and information are generated using the liver CT segmentation/CNN. Man-in-the-middle attacks on DICOM streams or picture tampering may be indicated by any variations (improbable anatomy, missing series, altered pixel statistics). [13].

Table 2: Model Architectures for FL-Based Security

Model Type	Application in Healthcare Security	Advantage
CNN	Network traffic classification	High feature extraction accuracy
RNN / LSTM	Sequential packet analysis	Captures temporal attack patterns
Autoencoders	Unsupervised anomaly detection	Detects zero-day threats
Graph Neural Networks (GNNs)	Network topology threat modeling	Identifies lateral movement

B. Federated Security Workflow

Workflow overview:

1. Hospitals train their own local security models based on their local traffic data.
2. The updates to these models are encrypted and transmitted securely.
3. A central aggregation server computes the updates securely through averaging.
4. The improved global model is then redistributed for the next round of training.

In addition to safeguarding vital network data locally, this recurrent loop helps us spot issues among healthcare providers [14].

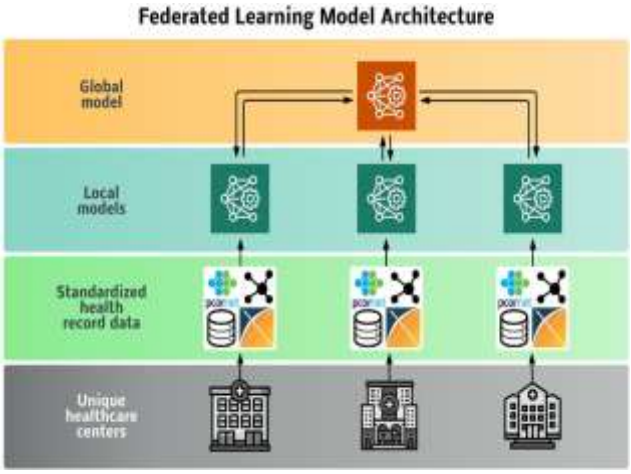

Figure 2: Federated Learning Model Architecture

V. System Architecture Proposal

This section describes a secure and scalable Federated Learning framework that is intended to ensure privacy while facilitating collaboration on network security among scattered healthcare providers [15]. The framework focuses on compliance, resilience to cyber threats, and effective sharing of collaborative intelligence.

A. Hierarchical Federated Framework

For addressing the issues of scalability and diverse data, it is recommended to have a tiered federated system [16]. The hospitals are grouped based on geographical regions or similar network features. For each group, there is a regional aggregation server that manages the local updates, and a central health authority that manages the global updates of the model.

A three-tier architecture maintains efficiency and concentration on patient care networks.

1. **Tier 1 – Local Layer:** hospital-level intrusion detection systems are trained on internal network logs, IoT data, and firewall logs.
2. **Tier 2—Regional Aggregation:** To provide a regional perspective without revealing the data, regional servers gather and safely average the institutions' encrypted updates.
3. **Tier 3-Global Coordination:** A central orchestrator integrates regional models to produce a security paradigm that works effectively globally.

With this multi-tier approach, communication overhead is minimized and faster model convergence is guaranteed, even if the healthcare data is not IID [17].

B. Secure Federated Protocol

Security mechanisms are:

- **Secure Aggregation:** prevents reconstruction of individual hospital updates [18].

International Journal of Science and Engineering Applications
Volume 15-Issue 04, 07 – 15, 2026, ISSN:- 2319 - 7560
DOI: 10.7753/IJSEA1504.1003

- **Differential Privacy (DP):** adds controlled noise to gradients.
- **End-to-End Encryption (TLS):** protects parameter transmission.
- **Robust Aggregation (e.g., Krum, Median):** prevents model poisoning attacks.

C. Edge–Cloud Integration

Real-time training and fault detection are carried out via the edge servers of the hospital networks. Audit compliance, logging, and global orchestration are managed by the cloud's federated coordinator [19].

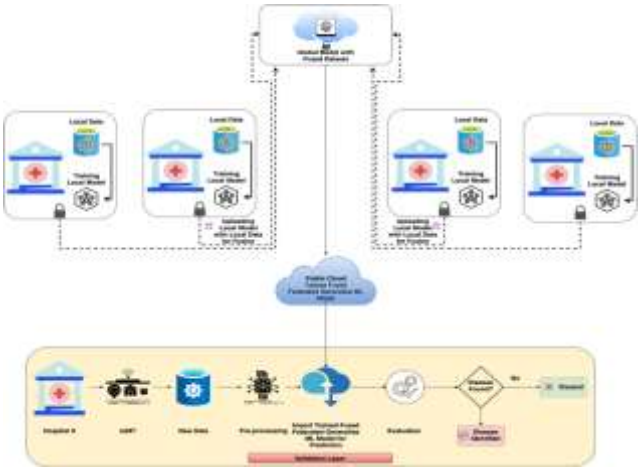

Figure 3: Proposed Architecture

VI. Privacy Preservation and Security Analysis

Federated Learning (FL) enhances cybersecurity in the healthcare industry while maintaining complete privacy [20]. If the level of protection is insufficient, the model updates provided may contain sensitive information even if the original data is still in each organization. Healthcare businesses must use both effective threat mitigation techniques and creative privacy-preserving methods to guarantee the security of their systems.

A. Privacy-Enhancing Techniques

1. **Differential Privacy (DP):** To reduce the likelihood that patient data may be mathematically deduced, we introduce noise to the local gradients prior to transmission. The privacy measure is tracked by the epsilon (\(\epsilon\)) number.
2. **Secure Multi-Party Computation (SMPC):** The model updates are broken into cryptographic shares such that not even the aggregator can deduce the parameters.
3. **Homomorphic Encryption (HE):** Enables computations to be performed on the encrypted updates, such that nothing is leaked during aggregation without decrypting [21].
4. **Secure Aggregation Protocols:** Ensure that the server coordinating the process can only access the final aggregated output and not the individual updates.

B. Threat Models and Countermeasures

FL systems in the healthcare industry need to be able to protect themselves from a variety of threat sources, including both internal and external users [22]. Some of these clients try to mislead the global model because they disagree with it.

Table 3: Threat Models and Countermeasures

Threat Type	Description	Mitigation Strategy
Model Poisoning	Malicious client injects harmful updates	Robust aggregation (Krum, Median)
Membership Inference	Attacker infers presence of patient data	Differential Privacy
Gradient Leakage	Reconstruction of local data from updates	Encryption + Secure Aggregation
Communication Interception	Man-in-the-middle attacks	TLS & End-to-End Encryption

C. Security-Privacy Trade-off

A trade-off between privacy and model accuracy might be necessary for lower ε values [23]. In order to maintain the safety of healthcare networks, the model's designers had to find the best possible balance between detection rate, communication effectiveness, and regulations.

VII. Experimental Evaluation

This section will examine the privacy and network security advantages of Federated Learning (FL), as well as how well it protects privacy and improves the security of healthcare networks [24]. Federated models compete with centralized models and models that are only used in one location in the testing.

A. Experimental Setup

A system with a few hospitals acting as federated client nodes is envisioned in the proposed study. Each hospital keeps its own collection of network traffic logs, firewall event logs, and IoT telemetry information. The global model is maintained by the central server. FedAvg is used in conjunction with secure aggregation to safeguard the global parameters [25].

International Journal of Science and Engineering Applications
Volume 15-Issue 04, 07 – 15, 2026, ISSN:- 2319 - 7560
DOI: 10.7753/IJSEA1504.1003

a) Important points:

1. **Clients:** 10-20 federated hospitals
2. **Models:** Convolutional Neural Network (CNN) for traffic classification, and Autoencoder for anomaly detection [26].
3. **Privacy:** Differential Privacy with carefully chosen values of ε.
4. **Training epochs:** 100-200 communication rounds

B. Baseline Comparisons

Three different layouts are being examined.

1. **Centralized Learning:** all data is centralized on one server.
2. **Local Learning:** each hospital learns from their own data.
3. **Federated Learning:** each group learns together in a decentralized fashion.

Accuracy, F1-score, detection latency, communication overhead, and privacy leakage are among the assessment criteria [27].

C. Results and Performance Analysis

The results demonstrate that federated learning techniques are significantly better than local models but almost as good at locating things as centralized models. Even though the noise added for privacy protection significantly lowers accuracy, federated models perform well in a range of healthcare scenarios. Due to regular aggregation, communication overhead is kept low [28].

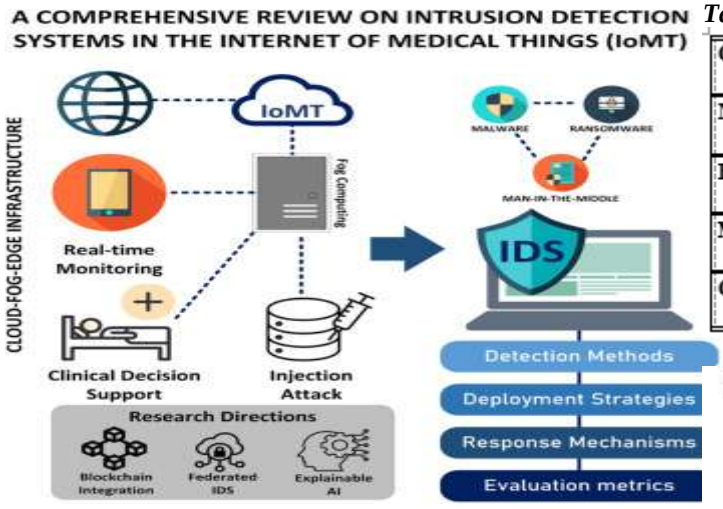

Figure 4: Detection System in The Internet of Medical Things (IOMT)

VIII. Challenges and Future Directions

Federated Learning (FL) is a great way to keep healthcare networks private, but when it is used by multiple healthcare providers, it presents a number of organizational, technological, and legal issues [29].

A. Key Challenges

1. **Data heterogeneity (non-IID data):** Hospitals differ in terms of patients, devices, and network settings. If the data is not spread uniformly, it could take longer to train a model and result in a less effective global model [30].
2. **Communication Overhead:** Exchanging model parameters from time to time between hospitals consumes bandwidth, which becomes more problematic for deep neural networks.
3. **Security of Federated Updates:** Malicious users may attempt to poison or introduce backdoors in the model via federated updates [31].
4. **Regulatory and Governance Complexity:** Global collaborations are required to comply with regulations such as HIPAA and GDPR [32].

B. Future Research Directions

1. Adaptive Federated Optimization (FedProx, Clustered FL) to deal with heterogeneity in hospitals
2. Model compression and sparse updates to reduce communication overhead
3. Blockchain-based audit trails to provide accountability
4. Explainable Federated AI (XAI) for regulatory purposes
5. Federated threat intelligence sharing frameworks

Table 4: Challenges and Mitigation

Challenge	Impact	Potential Solution
Non-IID Data	Slow convergence	Clustered FL
High Communication Cost	Latency	Model compression
Model Poisoning	Reduced accuracy	Robust aggregation
Compliance Barriers	Legal risks	Governance frameworks

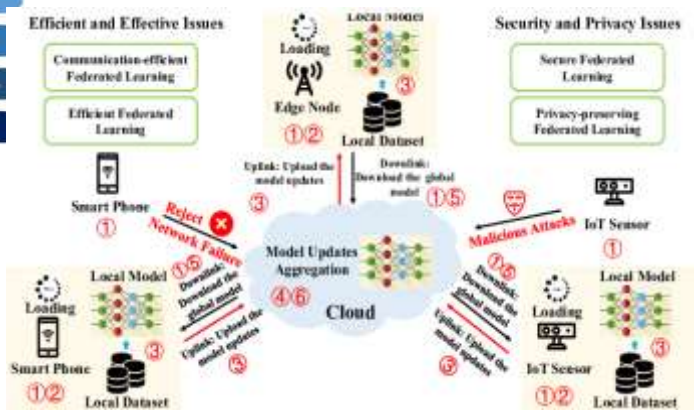

Figure 5: Future Evolution Roadmap

IX. CONCLUSION

A rising number of hospitals and medical organizations are experiencing ransomware attacks, data breaches, and complex hacking attempts. Because it requires a lot of data in one place, centralized machine learning for cybersecurity is good at identifying dangers, but it also presents privacy, legal, and practical issues. Federated learning (FL), which enables medical institutions to work together and improve their defenses without disclosing patient or network data, is a big step forward.

Federated learning uses encryption, safe aggregation, and differential privacy to spread training across several nodes. In compliance with regulations like HIPAA and GDPR, this facilitates the identification of hazards. The suggested hierarchical federated design shows how several healthcare organizations can collaborate to develop dependable anomaly and intrusion detection systems while maintaining data ownership.

It has numerous problems, though, such as transferring too much data, having too many distinct kinds of data, and being easily hacked. Strong optimization, explainable AI, and safe federated governance will be more beneficial. In conclusion, Federated Learning is a scalable and privacy-friendly foundation for next-generation healthcare network security systems.

REFERENCES

[1] Ting, Daniel S., Dinesh V. Gunasekeran, Louisa Wickham, and Tien Yin Wong. "Next generation telemedicine platforms to screen and triage." *British Journal of Ophthalmology* 104, no. 3 (2020): 299-300.

[2] Said, Abdelmlak, Aymen Yahyaoui, and Takoua Abdellatif. "HIPAA and GDPR compliance in IoT healthcare systems." In *International conference on model and data engineering*, pp. 198-209. Cham: Springer Nature Switzerland, 2023.

[3] Ray, Niranjan K., Deepak Puthal, and Dhruva Ghai. "Federated learning." *IEEE Consumer Electronics Magazine* 10, no. 6 (2021): 106-107.

[4] Fanelli, Simone, Lorenzo Pratici, Fiorella Pia Salvatore, Chiara Carolina Donelli, and Antonello Zangrandi. "Big data analysis for decision-making processes: challenges and opportunities for the management of health-care organizations." *Management Research Review* 46, no. 3 (2023): 369-389.

[5] An, Tianbo, Leyu Ma, Wei Wang, Yunfan Yang, Jingrui Wang, and Yueren Chen. "Consideration of FedProx in privacy protection." *Electronics* 12, no. 20 (2023): 4364.

[6] Isola, Sasank, and Yasir Al Khalili. "Protected health information." In *StatPearls [Internet]*. StatPearls Publishing, 2023.

[7] Kan, Karen, and Wilton C. Levine. "Infusion pumps." In *Anesthesia equipment*, pp. 351-367. WB Saunders, 2021.

[8] Rajasekar, Vani, J. Premalatha, and Rajesh Kumar Dhanaraj. "Security analytics." In *System Assurances*, pp. 333-354. Academic Press, 2022.

[9] Mohammed, Naveed Uddin, Zubair Ahmed Mohammed, Shravan Kumar Reddy Gunda, Akheel Mohammed, and Moin Uddin Khaja. "Networking with AI: Optimizing Network Planning, Management, and Security through the medium of Artificial Intelligence."

[10] Zhang, Junpeng, Hui Zhu, Fengwei Wang, Jiaqi Zhao, Qi Xu, and Hui Li. "Security and privacy threats to federated learning: Issues, methods, and challenges." *Security and Communication Networks* 2022, no. 1 (2022): 2886795.

[11] Belenguer, Aitor, Jose A. Pascual, and Javier Navaridas. "A review of federated learning applications in intrusion detection systems." *Computer Networks* 258 (2025): 111023.

[12] Madani, Houria, Noura Ouerdi, Ahmed Boumesaoud, and Abdelmalek Azizi. "Classification of ransomware using different types of neural networks." *Scientific Reports* 12, no. 1 (2022): 4770.

[13] R. Thatikonda, S. Kadakadiyavar, A. Padthe and M. G K, "Diagnosis of Liver Tumor from CT Scan Images using Deep Segmentation Network with CMBOA based CNN," 2023 IEEE 3rd Mysore Sub Section International Conference (MysuruCon), HASSAN, India, 2023, pp. 1-8, doi: 10.1109/MysuruCon59703.2023.10396968.

[14] Mehanoor, Syeda Husna, and Shakeel Ahmed. "Safeguarding data and ensuring security in digital healthcare." In *Transforming Gender-Based Healthcare with AI and Machine Learning*, pp. 160-184. CRC Press, 2024.

[15] Chaves, António, Larissa Montenegro, Hugo Peixoto, António Abelha, Luís Gomes, and José Machado. "Intelligent systems in healthcare: an architecture proposal." In *International Symposium on Ambient Intelligence*, pp. 230-238. Cham: Springer Nature Switzerland, 2023.

[16] Deng, Yongheng, Feng Lyu, Tengxi Xia, Yuezhi Zhou, Yaoxue Zhang, Ju Ren, and Yuanyuan Yang. "A communication-efficient hierarchical federated learning framework via shaping data distribution at edge." *IEEE/ACM Transactions on Networking* 32, no. 3 (2024): 2600-2615.

[17] Chen, Kun-Yi, Chi-Ren Shyu, Yuan-Yu Tsai, William I. Baskett, Chi-Yu Chang, Che-Yi Chou, Jeffrey JP Tsai, and Zon-Yin Shae. "Effective non-IID degree estimation for robust federated learning in healthcare datasets." *Journal of Healthcare Informatics Research* 9, no. 3 (2025): 437-464.

[18] Fereidooni, Hossein, Samuel Marchal, Markus Miettinen, Azalia Mirhoseini, Helen Möllering, Thien Duc Nguyen, Phillip Rieger et al. "SAFELearn: Secure aggregation for private federated learning." In *2021 IEEE security and privacy workshops (SPW)*, pp. 56-62. IEEE, 2021.

[19] Ayachi, Messaouda, Hassina Nacer, and Hachem Slimani. "Cooperative game approach to form overlapping cloud federation based on inter-cloud architecture." *Cluster Computing* 24, no. 2 (2021): 1551-1577.

[20] Ansari, Meraj Farheen. "Redefining Cybersecurity: Strategic Integration of Artificial Intelligence for Proactive Threat Defense and Ethical Resilience."

[21] Cheon, Jung Hee, Anamaria Costache, Radames Cruz Moreno, Wei Dai, Nicolas Gama, Mariya Georgieva, Shai Halevi et al. "Introduction to homomorphic encryption and schemes." In *Protecting Privacy through Homomorphic Encryption*, pp. 3-28. Cham: Springer International Publishing, 2022.

[22] Ferrag, Mohamed Amine, Leandros Maglaras, Abdelouahid Derhab, and Helge Janicke. "Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues." *Telecommunication Systems* 73, no. 2 (2020): 317-348.

[23] Akinsanmi, Titi, and Aishat Salami. "Evaluating the trade-off between privacy, public health safety, and digital security in a pandemic." *Data & Policy* 3 (2021): e27.

[24] Li, Jianbin, Xin Tong, Jinwei Liu, and Long Cheng. "An efficient federated learning system for network intrusion detection." *IEEE Systems Journal* 17, no. 2 (2023): 2455-2464.

[25] Mohammed, Akheel, Zubair Ahmed Mohammed, Naveed Uddin Mohammed, Shravan Kumar Gunda, Mohammed Azmath Ansari, and Mohd Abdul Raheem. "AI-NATIVE WIRELESS NETWORKS: TRANSFORMING CONNECTIVITY, EFFICIENCY, AND AUTONOMY FOR 5G/6G AND BEYOND

[26] Ketkar, Nikhil, and Jojo Moolayil. "Convolutional neural networks." In *Deep learning with Python: learn best practices of deep learning models with PyTorch*, pp. 197-242. Berkeley, CA: Apress, 2021.

[27] Kang, Yoojin, Eunna Jang, Jungho Im, and Chungeun Kwon. "A deep learning model using geostationary satellite data for forest fire detection with reduced detection latency." *GIScience & Remote Sensing* 59, no. 1 (2022): 2019-2035.

[28] Bansal, Shivangi, Suraj Rajesh Rajesh Karpe, Sujayaraj Samuel Jayakumar, and Swarup Kumar Bisoi. "Investigation of scenario-

based simulation for communication skills development in healthcare education." *Health Leadership and Quality of Life* 1 (2022): 64.

[29] Zhavoronkova, Natalya G., and Vyacheslav B. Agafonov. "Organizational and legal problems of the program for the development of genetic technologies implementation." *RUDN Journal of Law* 25, no. 4 (2021): 901-916.

[30] Raheem, M. A., & Ansari, M. A. Open Access Publication| ISSN: 2582-0176.

[31] Nguyen, Truc, and My T. Thai. "Preserving privacy and security in federated learning." *IEEE/ACM Transactions on Networking* 32, no. 1 (2023): 833-843.

[32] Syeda, Mrs Salma. "REGULATION COMPLEXITY AND COSTS OF GOVERNANCE." *Asian Journal of Multidimensional Research (AJMR)* (2022).194.