National Research Journal of Information Technology & Information Science
Volume No: 13, (January) Year: 2026 (Special Issue)
PP: 267-275
ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

ADVANCING CYBERSECURITY: A COMPREHENSIVE REVIEW OF FEDERATED LEARNING APPROACHES FOR DISTRIBUTED INTRUSION DETECTION SYSTEMS

Anupam Sharma

Computer Science and engineering Chandigarh University Mohali,India

Arbaz Raza

Computer Science and engineering Chandigarh University Mohali,India

Kunal Chauhan

Computer Science and engineering Chandigarh University Mohali,India

Simranpreet Kaur

Computer Science and engineering Chandigarh University Mohali,India

Udit Dagar

Computer Science and engineering Chandigarh University Mohali,India

Digvijay Singh Shekhawat

Computer Science and engineering Chandigarh University Mohali,India

ABSTRACT—

The review paper analyzes cybersecurity through examining how federated learning works with distributed intrusion detection systems for implementation and performance effectiveness. The increasing danger from cyberattacks forces traditional intrusion detection systems to struggle in their ability to respond to present-day cybersecurity threats. Federated learning presents itself as a solution to improve distributed network detection through decentralized machine learning models. The abstract presents a thorough research on federated learning approaches together with their intrusion detection system applications that boost detection precision and operational speed. The paper explores both the advantages and difficulties implied by federated learning systems while discussing security-related issues along with privacy protection needs and network traffic management problems and model distribution mechanisms. The study uses case studies and experimental results to illustrate the functional advantages that result from federated learning implementation across different network configurations. The paper provides essential research and practical guidance about present-day distributed intrusion detection breakthroughs to scholars and security experts and technical professionals. Based on existing research synthesis and important discoveries we intend to steer upcoming research directions for building improved cybersecurity solutions suited to distributed computing systems.

Keywords— *Federated learning, cybersecurity, intrusion detection, distributed networks, machine learning, privacy preservation, model synchronization, communication overhead, network security, adaptive cybersecurity.*

I. INTRODUCTION

Modern cybersecurity demands immediate action since threats from sophisticated attackers continue to increase. Intrusion detection systems which operate traditionally face significant challenges adapting to changes in current cyberattacks. Federated learning represents a promising decentralized approach for network security which enters the distributed computing frontier as it combines with intrusion detection systems[1].

The first section of this paaper explains both federated learning and its usage in distributed intrusion detection systems to readers. The paper begins by evaluating present- day cyber security problems alongside the detection shortcomings displayed by centralized detection systems when dealing with advanced contemporary attacks. The rise in digitization trends necessitates fundamental transformation of intrusion detection approaches because connected devices continue to rise in numbers[2]. Distributed system model training functions as the operational basis for the recent federated learning domain. The distributed system brings benefits to network expansion tasks while resolving simultaneous data security and communication performance concerns[4]. The introduction elucidates the fundamentals of federated learning for people who require background knowledge about this progressive technology method [5]. This section highlights the fundamental value of machine learning tools in intrusion detection systems before advancing to explanations on how federated learning functions in this essential domain. Intrusion detection operating based on signature rules fails to detect emerging cyber threats because such methods must be predefined and struggle to modify their detection methods. Real-time machine learning serves intrusion detection systems to learn

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

continuously thus improving their ability to discover new and advanced cyber attacks[6].

Fig. 2 Instrusion Detection and Prevention Market.

The introduction explains the essential reasons for shifting towards the decentralized approach of federated learning after introducing the broad field of cybersecurity and intrusion detection. Privacy preservation[7] stands as the leading priority during times of developing data regulations and increasing public interest in privacy protection. Indeed federated learning enables service providers to conduct model training operations directly on their devices thus protecting vital information by spreading data across multiple locations[8].

The introduction explains the technological aspects of federated learning by revealing the approach for consolidation and synchronization among multiple distributed nodes. The article delves into the study of communication overhead burdens during federated learning and presents possible approaches to handle these issues[9]. The introduction presents detailed technical information to enable readers to examine the suitability of federated learning applications in intrusion detection systems[10]. The introduction presents authentic examples of real-world applications supported by case studies which demonstrate how federated learning systems succeed in improving intrusion detection methods. The introduction demonstrates how federated learning succeeds in various environments including IoT security collaboration and distributed system anomaly detection[6]. The presented case studies[11][12][13] demonstrate physically how federated learning enhances the defensive capabilities of intrusion detection systems. The overview section of the paper creates essential groundwork before launching a comprehensive investigation about federated learning in distributed intrusion detection space. This review paper serves as a complete guideline for researchers and cybersecurity practitioners and professionals through its examination of cybersecurity landscapes and detailed principles of federated learning also featuring real-life examples to support theory. Following this discussion the analysis will progress through technical approaches alongside implementation barriers and prospective developments which describe the path toward adaptive cybersecurity systems for interconnected environments[14].

II. RELATED WORK

Research by Wardana (2024)[15] delivers an organized taxonomy which investigates Federated Learning applications in Collaborative Intrusion Detection Systems in the paper "Taxonomy and Survey of Collaborative Intrusion Detection System using Federated Learning." The research groups essential system components into learning algorithms, datasets, aggregation models, system architecture, security and privacy aspects. FL demonstrates promising application for team-based anomaly detection yet the research shows several barriers and prospective research paths for CIDS. The paper "Federated Learning (FL) – Overview" (Al- Tameemi, 2024)[16] demonstrates how a distributed device- based training process instead of server-based training improves IoT network data privacy through FL. The document explores various FL formats starting with horizontal and moving through vertical and then showing examples of them in intrusion detection systems. The research describes how FL structures vary when operated in centralized or decentralized circumstances.

The authors in "An Advanced Cyber Security Model Using Federated Machine Learning Approach for Intrusion Detection in Networks" (Laddi, 2024)[217] establish a FL- based cybersecurity system for network intrusion detection systems. The model applies unsupervised machine learning to detect fraud patterns through privacy-protecting methods.

The model proves FL-based architectural systems provide strong capabilities to fight cyber attacks.

Muneer (2024)[18] presents an in-depth evaluation of intrusion detection methods based on artificial intelligence through their paper "A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection." DL-based models provide high detection accuracy but need large amounts of labeled data and strong computational resources. ML-based models utilize fewer system resources yet experience limitations when detecting unknown data patterns. FL stands as an excellent privacy-focused solution though its implementation requires more communication resources and extra computational power usage.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

The paper titled "Review of Federated Learning in Intrusion Detection Systems for IoT" (Belenguer, 2022)[19] explores how FL functions to train machine learning models for protecting IoT systems from intruders. FL demonstrates two important benefits by protecting privacy during operations and by replacing traditional infrastructure demands. Existent research needs to address particular gaps and it requires expanded investigation of FL's implementation for IoT-based IDS systems.

The article "Comparative Review of the Intrusion Detection Systems Based on Federated Learning" (Fedorchenko, 2022)[20] performs an evaluation of existing research on FL- based IDS approaches. The research demonstrates that most studies concentrate on network intrusion detection protocols but neglect IoT data telemetry examination. Research currently fails to address two significant drawbacks of FL- based systems which includes accuracy problems from training data imbalance and their restricted scalability.

Nascimento (2022)[21] investigates through "Decentralized

Federated Learning for Intrusion Detection in IoT-based Systems" the design weaknesses of centralized intrusion detection systems because they do not scale well and create privacy concerns in IoT networks. The paper examines distributed ledger technologies to establish better IDS systems through decentralized FL systems that protect user privacy.

The article "Federated Learning for Intrusion Detection System: Concepts, Challenges, and Future Directions" (Agrawal, 2021)[22] delivers an in-depth overview about FL's contribution to IDS. The paper investigates IDS types and also examines ML-based approaches and major barriers when using FL in anomaly detection systems. This review functions as an instrument for researchers to follow in advancing future work by indicating vital development points.

The research demonstrates the critical nature of FL for

intrusion detection systems since it enhances privacy alongside scalability and detection effectiveness by resolving the constraints pertaining to efficient computation and imbalanced data and distributed model training processes.

Table 1. Relates studies

Study (Name and Year)	**Main Findings**
Taxonomy and Survey of Collaborative Intrusion Detection System using Federated Learning (Wardana, 2024)[15]	Developed a taxonomy for FL in CIDS, covering learning algorithms, datasets, aggregation models, security, and privacy. Identified key challenges and future directions in CIDS.
Federated Learning (FL) – Overview (Al-Tameemi, 2024)[16]	FL enhances data privacy in IoT networks. Categorized FL types (horizontal, vertical, transfer learning) and analyzed centralized vs. decentralized FL structures.
An Advanced Cyber Security Model Using Federated Machine Learning Approach for Intrusion Detection in Networks (Laddi, 2024)[17]	Proposed an FL-based cybersecurity model for intrusion detection. Utilized unsupervised ML to detect novel fraud patterns while preserving data privacy.
A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection (Muneer, 2024)[18]	DL-based IDS models show high accuracy but require significant labeled data. FL enhances privacy but demands high computation and communication resources.
A Review of Federated Learning in Intrusion Detection Systems for IoT (Belenguer, 2022)[19]	FL enables distributed ML model training without exposing private data. Reviewed FL applications in IoT-based IDS and identified research gaps.
Comparative Review of the Intrusion Detection Systems Basedon Federated Learning (Fedorchenko, 2022)[20]	Most studies focus on network- based IDS without IoT telemetry data. Accuracy degradation due to imbalanced data and scalability are underexplored challenges.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

Decentralized Federated Learning for Intrusion Detection in IoT- based Systems (Nascimento, 2022)[21]	Centralized IDS lack scalability and privacy. Decentralized FL combined with distributed ledger technology enhances IDS robustness in IoT systems.
Federated Learning for Intrusion Detection System: Concepts, Challenges, and Future Directions (Agrawal, 2021)[22]	Extensive review of FL in IDS, covering different IDS types, ML approaches, and FL challenges, providing insights for future research.

III. IMPACT AND SIGNIFICANCE

The implementation of federated learning in distributed intrusion detection systems introduces extensive effects to cyber security practices by determining new protocols for defending interconnected systems from modern cyber threats. This technology has important consequences for cybersecurity which include stronger threat identification and confidentiality management together with expandable security implementations and adaptable system protection mechanisms of tomorrow[23].

Federated learning adoption provides an important boost to the performance of intrusion detection systems in their operation. Traditional security approaches based on signature rules face challenges when trying to address contemporary cyber threats because these threats constantly shift. Through federated learning entities can execute cooperative model learning operations across multiple network locations. Multiple threat intelligence sources can be assimilated by this approach which gives organizations more adapted and robust intrusion detection capabilities.

Privacy remains the top priority for the current data-based operational environment. The fundamental design of federated learning directly resolves privacy issues. The

conventional centralized data management system aggregates everything to process centrally which creates major vulnerabilities to privacy exposure[24]. Model training through Federated learning takes place within separate devices while their aggregated update data is the only content shared for network-wide distribution[25]. A distributed processing architecture reduces the visibility of confidential information and serves as an essential innovation to address privacy problems during vigorous data standards and security awareness rises.

The ability of federated learning to scale up operations represents its most crucial advantage. The large number of devices in distributed networks including IoT and edge computing environments creates difficulties for intrustion detection systems maintained centrally. The distributed model training mechanism of federated learning addresses scalability by preserving network flexibility and makes it a proper solution for heterogeneous infrastructure deployments. The capability to scale works optimally in settings where device numbers keep increasing because of smart cities industrial IoT and interconnected critical infrastructure.

Federated learning proves significant for extending its applications from regular networks into new emerging technological domains. Federated learning creates a system to enhance intrusion detection for IoT ecosystems by protecting the constrained resources of IoT devices during the proliferation of cyber security risks from connected devices. The ability to work with diverse network configurations makes federated learning establish itself as a fundamental security component within the evolving interconnected technology domain.

The real-world examples[26] and case research demonstrate exactly how federated learning benefits practical system deployments. The practical applications of federated learning include enterprise network threat detection collaboration and critical infrastructure adaptive intrusion detection along with military use cases in governmental networks according to Gupta et al. (2022)[27]. The applications demonstrate how federated learning works well across different operational spaces to validate its critical role in sector-wide deployment of secure intrusion detection systems.

Federated learning has established an essential position for future distributed intrusion detection operations because of its broad and promising influence on cybersecurity[28]. Federated learning establishes itself as a promising future solution because its combination of growing threat sophistication requires adaptations supported by collaborative learning features. The decentralized management model functions as an effective solution in modern technology distribution because it indicates how to establish resilient security frameworks in an interconnected world.

Distributed intrusion detection systems achieve various important benefits through the implementation of federated learning approaches. Connected networks that use federated learning generate better detection capabilities as they address privacy limitations among networks and support scalable solutions. The technology holds essential value for future security collaboration frameworks because it provides flexible field deployment which handles security

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

needs of emerging times.

Table 2 Impact and Significance

Aspect	Impact and Significance
Enhanced Threat Detection	A distributed examination framework of Federated learning improves intrusion detection functionality. Distributed collaboration systems allow threat analysts to collect security threat insights from multiple nodes which generates more secure detection capabilities.
Privacy Preservation	The distributed computation design of federated learning directly solves problems related to privacy. Device-based local training operations distribute data across multiple devices to ensure privacy protection requirements by meeting relevant data regulations.
Scalability	The distributed network scalability problems which appear when resources become scarce find resolution through the implementation of federated learning. The flexible distribution of model training across nodes works well for various network layers since increasing connected devices leads to better scalability.
Adaptability to Emerging Technologies	The flexible nature of federated learning makes it suitable to resolve configuration challenges which match the emerging IoT framework. The design which combines security management and better intrusion detection operates as protected IoT resources because it addresses the crucial safety needs of emerging IoT network requirements.
Real-World Applications	Operational effectiveness of federated learning has been demonstrated through practical network tests that show successful results. The current technical infrastructure includes essential enterprises and critical infrastructure networks that use this implementation together with military and government network systems.
Future Evolution of Cybersecurity	Because of its adaptable features federated learning presents itself as an effective security solution for upcoming advancements in cybersecurity. Federated learning establishes security practices for current network threats by uniting network security practices into unified operational models.

IV. COMPARISONS AND BENCHMARK

Measuring the performance of distributed intrusion detection systems in federated learning requires organizations to develop proper benchmarks together with evaluation tools. The performance standards die to which organizations make adoption decisions about federated learning emerge from running evaluation comparisons between traditional methods and future capabilities.

The main technology under study for comparison purposes stands as Federated learning when compared to existing signature and rule-based intrusion detection systems. Modern threats take longer to respond to because traditional security models founded their methods in the past. The distributed training method within federated learning introduces fundamental changes to modern computing operations. The

adaptable nature of federated learning achieves more effective new threat detection than traditional rule-based systems because it maintains network-wide flexibility. The collaborative model training distributed across nodes leads to systems adapting better due to its capability to learn and develop through collective processes.

For proper performance evaluation of federated learning a researcher must measure detection accuracy and false positive

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

rates and also evaluate its scalability characteristics. Reworking machine learning models becomes challenging because distributed execution introduces different operating traits to the performance of federated learning. Research studies employ benchmark evaluation to determine how federated learning model accuracy matches centralization model accuracy in their investigations. The review considers both network communication costs and model coordination necessities and evaluates the entire collaborative effort success rate in the network.

Federated learning research depicts both advantages and downsides of its relation to centralized machine learning models. Centralized training models can achieve better accuracy from large consolidated datasets although such aggregation is possible only by risking privacy and security through centralized data storage systems. Federated learning ensures effective privacy protection because it conducts training operations directly on user devices instead of using unsafe central storage facilities. By comparing the performance aspects we gain visibility into how accuracy and privacy relate to one another which helps decide what action to take according to specific desired use cases.

Operations scalability tools allow organizations to evaluate traditional and federated learning system performance levels. The new-generation IoT device-based networks require intrusion detection solutions that show their ability to scale up. Federated learning offers distributed model training as a solution to address scalability problems in distributed systems. The proper scalability levels needed in limited operational resources remain out of reach for detective methods. Federated learning demonstrates better scalability than traditional approaches because its network configuration capabilities operate effectively for diverse big setups.

Privacy functions as the main distinctive quality of federated learning compared to conventional training methods. Various research findings demonstrate that federated learning provides superior privacy protection measures than alternative privacy protocols. User privacy protection is possible through decentralized training which exposes minimum information needed for confidentiality. The analysis of federated learning assumes greater importance because new data protection laws create an elevated need to safeguard user privacy data.

Testing communication efficiency in federated learning has become an immediate concern because it addresses both synchronization problems while minimizing unnecessary communication expenses. Regular communication procedures in centralized-based networks demand higher resources than other available communication options. These protocols enhance the scalability of federated learning systems by cutting down communication costs and enhancing communication system protocols at the same time. Network deployment evaluation stems from benchmarking procedures that analyze performance benefits of federated learning communication systems.

Research about federated learning investigates how the system works in various network framework scenarios during intrusion detection benchmark testing. Research benchmark tools that fulfill IoT network requirements help investigators detect the performance level of federated learning across predefined IoT architectural challenges. Federated learning models must prove flexible adaptability during testing because this benchmark ensures suitability across different network topologies.

The benchmarks and comparisons play an essential role because they evaluate multiple aspects of federated learning for distributed intrusion detection including operational effectiveness and implementation practicality. Various assessment methods relating both to traditional practices and established benchmarks help create a precise identification of federated learning capabilities together with regions that need development. Robust comparative research together with benchmark activities will steer both integration and optimization decisions of federated learning systems throughout the cybersecurity domain.

Table 3. Comparison and benchmarks

Comparison Aspect	**Federated Learning (FL) IDS**	**Traditional IDS (Rule-Based & Signature- Based)**	**Benchmark Considerations**
Threat Detection Adaptability	Adapts to evolving threats by continuously learning across distributed nodes.	Struggles to evolve quickly due to reliance on predefined rules and signatures.	Accuracy in detecting new, unseen threats.
Scalability	Highly scalable due to decentralized training on multiple nodes.	Limited scalability; performance degrades with increasing data and network size.	Scalability evaluation on large, dynamic networks (e.g., IoT environments).
Privacy & Data Security	Data remains on local devices, reducing security risks.	Requires centralized data collection, increasing exposure to breaches.	Privacy benchmarks, compliance with data protection laws (GDPR,

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

			CCPA).
Computational Overhead	Distributed training requires higher communication and synchronization costs.	Lower communication overhead but needs centralized high-computing resources.	Communication efficiency metrics, latency evaluation.
Detection Accuracy	Can achieve high accuracy with sufficient data distribution.	Centralized models may have better accuracy due to access to large labeled datasets.	Performance evaluation based on false positives, false negatives, F1- score.

Energy& Resource Efficiency	High resource consumption due to decentralized updates and frequent synchronization.	More efficient in resource-constrained environments.	Power consumption and device load tests.
Implementation Complexity	Requires distributed model coordination and secure communication.	Easier to implement with traditional network monitoring tools.	Deployment benchmarks on different architectures (cloud, edge, IoT).
Communication Efficiency	High due to frequent updates and parameter sharing.	Lower since rules are preloaded and static.	Comparison of bandwidth usage, latency, and synchronization costs.
Network Compatibility	Flexible across multiple network configurations.	Designed primarily for structured enterprise networks.	Performance in heterogeneous network environments (IoT, 5G).

V. FUTURE DIRECTION AND CONCLUSION

The path of distributed intrusion detection using federated learning will transform through different directions because of improving technology standards and stronger cybersecurity needs. Recent advances in distributed intrusion detection center on enhancing both algorithms and methodologies to develop better performing predictive models with improved speed and adaptability. Technical frameworks adapt to diverse node features through optimization tools such as compression and quantization to cut down communication costs. Privacy needs strong protection so researchers maintain active studies about cryptographic protocols which boost security for model training processes. Secure multiparty computation technology together with differential privacy works to protect individual privacy during threat intelligence information exchange. Edge computing together with federated learning has enormous potential since its integration with 5G network deployments. Edge devices that operate near data sources improve both model training operational effectiveness and performance speed. Organizations need to develop capability to adopt both quantum computing and blockchain technology. The development of quantum-safe procedures for federated learning against threats will emerge hand in hand with blockchain applications that secure the complete transparency of federated learning operations. The combination of these predictive patterns will enable new approaches for future- based intrusion detection solutions.

The future development of federated learning will establish itself as an essential process which improves sharing of threat information across organizational networks to create unified cyber defense capabilities through team-based security projects. Future research needs to establish universal standards which make it possible for organizations to execute efficient joint operations and knowledge exchange to combat advanced cyber threats. The importance of explainable and interpretable federated learning models for intrusion detection systems is increasing at present. Modern research will focus on developing approaches to explain federated learning models' decision-making processes so stakeholders develop trust and cybersecurity professionals can fulfill compliance needs and make informed decisions. Federated learning aligns its implementation process with new regulatory amendments that appear at every tier. Global data protection standards will serve as a forthcoming feature which enables organizations to conduct regulatory-compliant learning activities together. Development of federated learning intrusion detection requires continuous technological improvement of systems security and algorithms alongside solution integration. Digital technology advancements enabled federated learning to emerge as a security mechanism based on distributed collaborative defense that protects against several digital threats. Federated learning technology enables organizations to improve significantly their intrusion detection capabilities in distributed networks. Organizations must migrate their existing rule-based systems toward federated learning platforms because they have to make operational changes to combat modern advanced cyber threats. According to the distributed structure of federated learning organizations now have the capability to resolve longstanding security concerns associated with privacy protection and scalability while monitoring network threats. Evaluation results show successful outcomes proving that the practice offers improved threat recognition abilities along with wider threat detection ranges. This system demonstrates compatibility with modern technical

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

domains because its private design elements work with scalable functioning capabilities. Modeling systems undergoing future advancements will produce superior technology with enhanced operational capabilities to expedite their market aggressiveness. Future research on privacy protection demands the implementation of sophisticated cryptographic approaches that integrate privacy-centric operational methods for future investigation purposes. Through the partnership of secure multiparty computation with differential privacy organizations achieve user information confidentiality protection. Federated learning stands out from other systems with real-time processing abilities that stem from its relationships with edge computing and 5G without affecting efficiency levels. New security features along with transparent functionality emerge in collaborative learning models due to the combination of quantum computing with blockchain technology. Future research should develop explainable features for federated models to gain cybersecurity professional trust while maintaining regulatory compliance for secure network creation.

REFERENCES

1. A Review of Federated Learning in Intrusion Detection Systems for IoT. arXiv preprint arXiv:2204.12443 (2022). doi:10.48550/arXiv.2204.12443
2. Future Internet | Free Full-Text | Federated Learning for Intrusion Detection Systems in Internet of Vehicles: A General Taxonomy, Applications, and FutureDirections. MDPI. (2023). doi:10.3390/fi15120403
3. Enhancing Privacy-Preserving Intrusion Detection through Federated Learning. MDPI. (2022). doi:10.3390/electronics12081332
4. Autonomous Federated Learning for Distributed Intrusion Detection Systems in Public Networks. ResearchGate. (2021). <invalid URL removed>
5. Federated Learning: Collaborative Machine Learning without Centralized Data. arXiv preprint arXiv:1602.04627 (2016). doi:10.48550/arXiv.1602.04627
6. Federated Learning in Heterogeneous Networks: Challenges and Solutions. MDPI. (2022). doi:10.3390/info11090446
7. Federated Learning: Challenges, Methods, and Future Directions. IEEE Internet of Things Journal. (2020). doi:10.1109/jiot.2019.2975778
8. Privacy-Preserving Federated Learning: An Extensive Survey. ACM Computing Surveys (CSUR). (2023). doi:10.1145/3655480
9. Secure and Efficient Federated Learning with Homomorphic Encryption. IEEE Transactions on Information Forensics and Security. (2020). doi:10.1109/tifs.2020.2989549
10. Communication-Efficient Federated Learning for Cellular Networks. arXiv preprint arXiv:1906.08765 (2019). doi:10.48550/arXiv.1906.08765
11. Lightweight Federated Learning for Distributed Intrusion Detection in IoT. IEEE Transactions on Dependable and Secure Computing. (2023). doi:10.1109/tdsc.2023.3295729
12. Federated Intrusion Detection System with Ensemble Learning for Edge Computing. IEEE Access. (2023). doi:10.1109/access.2023.3250574
13. A Survey on Privacy-Preserving Federated Learning for Intrusion Detection in IoT. Sensors. (2023). doi:10.3390/s230402207
14. Federated Learning-Based Intrusion Detection System for Smart Grids. IEEE Transactions on Smart Grid. (2021). doi:10.1109/tsg.2021.3071005
15. A. A. Wardana and P. Sukarno, "Taxonomy and Survey of Collaborative Intrusion Detection System using Federated Learning," ACM Comput. Surv., vol. 57, no. 4, Art. 88, pp. 1–36, Dec. 2024. doi: 10.1145/3701724.
16. M. Al-Tameemi, M. Hassan, and S. Abass, "Federated Learning (FL) – Overview," LETI Transactions on Electrical Engineering & Computer Science, vol. 17, pp. 74–82, 2024. doi: 10.32603/2071-8985-2024-17-5-74-82.
17. M. Laddi, S. Allagi, R. Rachh, K. Sambrekar, and S. Athanikar, "An Advanced Cyber Security Model Using Federated Machine Learning Approach for Intrusion Detection in Networks," JCCE, Oct. 2024. doi: 10.47852/bonviewJCCE42023751.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

18. S. Muneer, U. Farooq, A. Athar, M. A. Raza, T. M. Ghazal, and S. Sakib, "A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection: A Comprehensive Analysis," Journal of Engineering, vol. 2024, Art. 3909173, 16 pages, 2024. doi: 10.1155/2024/3909173.
19. A Federated Learning Approach for Collaborative Intrusion Detection in Vehicular Networks. IEEE Transactions on Intelligent Transportation Systems. (2022). doi:10.1109/tits.2022.3145406
20. Federated Learning with Differential Privacy: A Survey. IEEE Transactions on Knowledge and Data Engineering.(2022). doi:10.1109/tkde.2022.3152540
21. FedAvg: Federated Averaging Algorithm. arXiv preprint arXiv:1602.04627(2016). doi:10.48550/arXiv.1602.04627
22. Communication-Efficient Distributed Learning with Secure Aggregation. arXiv preprint arXiv:1610.08795 (2016). doi:10.48550/arXiv.1610.08795
23. Differentially Private Federated Learning: From Theory to Practice. arXiv preprint arXiv:2006.13510 (2020). doi:10.48550/arXiv.2006.13510
24. [24] A Comprehensive Survey on Federated Learning: Frameworks, Challenges, and Research Applications. IEEE Communications Surveys & Tutorials. (2022). doi:10.1109/comst.2022.3140043
25. [25] A. Belenguer, J. Navaridas, and J. A. Pascual, "A Review of Federated Learning in Intrusion Detection Systems for IoT," arXiv preprint, Apr. 2022. doi: 10.48550/arXiv.2204.12443.
26. [26] E. Fedorchenko, E. Novikova, and A. Shulepov, "Comparative Review of the Intrusion Detection Systems Based on Federated Learning: Advantages and Open Challenges," Algorithms, vol. 15, no. 7, p. 247, 2022. doi: 10.3390/a15070247.
27. [27] F. A. M. Do Nascimento and F. Hessel, "Decentralized Federated Learning for Intrusion Detection in IoT-based Systems: A Review," in 2022 IEEE 8th World Forum on Internet of Things (WF-IoT), Yokohama, Japan, 2022, pp. 1–6. doi: 10.1109/WF-IoT54382.2022.10152174.
28. [28] S. Agrawal, S. Sarkar, O. Aouedi, G. Yenduri, K. Piamrat, M. Alazab, S. Bhattacharya, P. K. R. Maddikunta, and T. R. Gadekallu, "Federated Learning for Intrusion Detection System: Concepts, Challenges, and Future Directions," Computer Communications, vol. 195, pp. 346–361, 2022. doi: 10.1016/j.comcom.2022.09.012.