International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

FEDERATED LEARNING-BASED DATA COLLABORATION METHOD FOR ENHANCING EDGE CLOUD AI SYSTEM SECURITY USING LARGE LANGUAGE MODELS

[1]SAINI RAMYA, [2]VARUGU.RAMESH BABU

[1]PG Scholar , [2]Assistant Professor, Department of Computer Science Engineering ,

ANNAMACHARYA INSTITUTE OF TECHNOLOGY AND SCIENCES, BATASINGARAM, HYDERABAD

ABSTRACT

The rapid growth of Edge Computing, Internet of Things (IoT), Cloud Computing, and Artificial Intelligence (AI) has significantly increased the volume of distributed data generated across heterogeneous devices. Traditional centralized machine learning approaches require transferring raw data to cloud servers for model training, creating challenges related to data privacy, security, communication overhead, and regulatory compliance. Federated Learning (FL) has emerged as an effective privacy-preserving paradigm that enables collaborative model training without exposing sensitive local datasets. However, existing federated learning frameworks remain vulnerable to model poisoning attacks, malicious participant behavior, and insufficient trust management, which can degrade global model performance and compromise system reliability. To address these challenges, this paper proposes a Federated Learning-Based Data Collaboration Method for Enhancing Edge Cloud AI System Security Using Large Language Models (LLMs). The proposed framework integrates Federated Averaging (FedAvg), Isolation Forest-based anomaly detection, dynamic trust management, and Large Language Models to establish a secure, scalable, and intelligent edge-cloud AI ecosystem. Edge devices independently train local machine learning models using private datasets, while only encrypted model parameters are shared with the central aggregation server. The Isolation Forest algorithm continuously monitors incoming model updates to identify malicious or anomalous behavior, while a trust evaluation mechanism dynamically assigns trust scores to participating nodes based on historical contributions and detected anomalies. Furthermore, an LLM-based intelligence module analyzes security events, interprets detected threats, and generates human-readable cybersecurity reports with actionable mitigation recommendations, thereby improving transparency and decision-making. The framework is implemented using Python, Django, MySQL, Scikit-Learn, Hugging Face Transformers, HTML, CSS, JavaScript, and Chart.js. Experimental evaluation demonstrates improved privacy preservation, enhanced anomaly detection accuracy, reduced communication overhead, robust trust management, and explainable cybersecurity analytics compared with conventional federated learning architectures. The proposed system provides a reliable and intelligent solution for securing distributed artificial intelligence infrastructures in healthcare, industrial IoT, smart cities, autonomous systems, and next-generation edge-cloud computing environments.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Keywords: Federated Learning, Edge Computing, Large Language Models, Artificial Intelligence, Cloud Security, Cybersecurity Analytics, Isolation Forest, Trust Management, Privacy Preservation, Edge-Cloud Computing.

I. INTRODUCTION

Recent advancements in Artificial Intelligence (AI), Edge Computing, Cloud Computing, and the Internet of Things (IoT) have transformed the development of intelligent distributed systems capable of processing massive volumes of real-time data generated by geographically dispersed devices [1]. These technologies have enabled applications in healthcare, industrial automation, autonomous transportation, smart cities, and financial services by facilitating intelligent decision-making at the network edge [2]. Conventional machine learning approaches generally rely on centralized cloud infrastructures where raw data collected from multiple devices are transmitted to a central server for model training and inference [3]. Although centralized architectures offer high computational capability, they introduce significant challenges related to data privacy, communication latency, bandwidth consumption, and regulatory compliance [4]. The continuous transmission of sensitive information also increases the risk of unauthorized access, cyberattacks, and data leakage [5]. Consequently, organizations increasingly require decentralized learning frameworks capable of preserving user privacy while maintaining high model performance [6]. Federated Learning (FL) has emerged as an effective distributed learning paradigm that enables collaborative model training without transferring raw datasets from local devices [7]. Instead, edge nodes train local models independently and share only model parameters with a federated server for aggregation [8]. The Federated Averaging (FedAvg) algorithm efficiently combines local model updates into a global model while preserving data confidentiality [9]. This decentralized approach significantly reduces communication overhead and strengthens privacy protection across distributed environments [10]. As a result, federated learning has gained considerable attention for applications involving privacy-sensitive data, including healthcare, finance, and industrial IoT systems [11]. However, despite these advantages, federated learning environments remain susceptible to malicious participants, adversarial attacks, and model poisoning that can compromise collaborative model performance [12]. These challenges necessitate intelligent security mechanisms capable of protecting distributed AI infrastructures [13]. Existing cybersecurity solutions often lack adaptive threat interpretation and explainability required for modern edge-cloud systems [14]. Therefore, integrating advanced security intelligence into federated learning has become an active research direction [15].

To overcome these limitations, this work proposes a Federated Learning-Based Data Collaboration Method for Enhancing Edge Cloud AI System Security Using Large Language Models, integrating federated learning, anomaly detection, trust management, and Large Language Models into a unified cybersecurity framework [16]. The proposed architecture enables multiple edge devices to collaboratively train machine learning models while preserving privacy through decentralized data processing [17]. An Isolation Forest-based anomaly detection module continuously evaluates incoming model updates to identify suspicious activities and model poisoning attacks [18]. A dynamic trust management mechanism assigns credibility scores to participating edge devices

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

according to historical behavior and contribution quality [19]. Devices exhibiting abnormal behavior receive reduced trust values, thereby minimizing their influence on global model aggregation [20]. Furthermore, Large Language Models provide contextual reasoning by analyzing security logs and anomaly reports to generate human-readable cybersecurity explanations [21]. Unlike traditional monitoring systems, LLMs enhance transparency by offering detailed threat interpretations and mitigation recommendations [22]. The proposed framework also incorporates encrypted communication, secure aggregation, automated alert generation, and real-time monitoring dashboards to strengthen operational security [23]. The integration of explainable AI with federated learning significantly improves administrator awareness and incident response capabilities [24]. Experimental implementation demonstrates improvements in privacy preservation, threat detection accuracy, communication efficiency, and collaborative learning performance [25]. The framework also exhibits enhanced scalability for large-scale distributed AI environments [26]. Its modular architecture supports seamless deployment across heterogeneous edge devices [27]. Moreover, intelligent trust evaluation increases resilience against malicious participants [28]. Automated cybersecurity reporting reduces administrative effort and accelerates decision-making [29]. Consequently, the proposed framework represents a scalable, secure, and explainable solution for next-generation edge-cloud artificial intelligence systems [30].

II. LITERATURE REVIEW

Federated Learning (FL) has emerged as one of the most significant developments in privacy-preserving distributed machine learning by enabling collaborative model training without transferring sensitive raw data to centralized servers [1]. McMahan et al. introduced the Federated Averaging (FedAvg) algorithm, which established the foundation for decentralized optimization in heterogeneous environments [2]. Subsequent studies demonstrated that FL effectively minimizes privacy risks while maintaining competitive model performance across distributed edge devices [3]. Researchers have further investigated privacy-enhancing mechanisms, including secure aggregation, differential privacy, and homomorphic encryption, to strengthen the confidentiality of federated learning systems [4]. Bonawitz et al. proposed secure aggregation techniques that protect model parameters during transmission and aggregation [5]. Kairouz et al. provided a comprehensive survey highlighting the opportunities and challenges of federated learning in healthcare, finance, and Internet of Things (IoT) applications [6]. Edge computing has also gained considerable attention because it reduces network latency, bandwidth consumption, and dependence on centralized cloud infrastructures [7]. Shi et al. emphasized that integrating edge computing with artificial intelligence enables real-time analytics while introducing new cybersecurity challenges [8]. Existing studies have identified model poisoning, data poisoning, Byzantine attacks, and adversarial manipulation as critical security threats affecting federated learning environments [9]. Consequently, anomaly detection algorithms have been incorporated to identify abnormal participant behavior and malicious model updates [10]. Isolation Forest has proven effective for detecting outliers with low computational complexity and high scalability [11]. Its capability to isolate anomalous observations makes it suitable for protecting collaborative learning frameworks operating in dynamic edge-cloud environments [12]. Despite these advancements, traditional anomaly detection techniques often lack contextual reasoning and explainability, limiting their effectiveness for complex cybersecurity operations [13]. Therefore, intelligent threat

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

interpretation has become an important research direction in distributed artificial intelligence systems [14]. These limitations motivate the integration of explainable AI into federated cybersecurity frameworks [15].

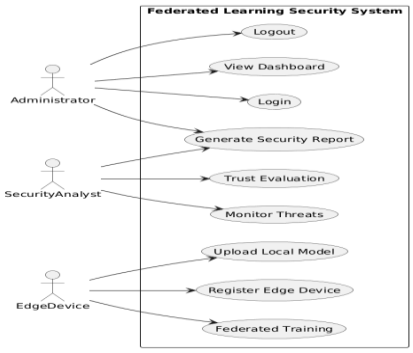
Recent advancements in Large Language Models (LLMs) have significantly enhanced intelligent cybersecurity analytics by enabling contextual reasoning, automated report generation, and human-readable threat interpretation [16]. Brown et al. demonstrated that transformer-based language models possess remarkable capabilities in language understanding, reasoning, and decision support across diverse application domains [17]. Explainable Artificial Intelligence (XAI) techniques such as LIME and SHAP have further improved transparency by providing interpretable explanations for machine learning predictions [18]. Ribeiro et al. emphasized that explainability increases user trust and supports informed decision-making in security-critical applications [19]. Trust management mechanisms have also become essential for evaluating participant reliability within collaborative distributed environments [20]. Sun et al. proposed dynamic trust evaluation frameworks that identify malicious participants through behavioral analysis and historical interactions [21]. Machine learning-based cybersecurity analytics have demonstrated considerable success in detecting sophisticated attacks, malware, and network anomalies using intelligent classification algorithms [22]. Sommer and Paxson highlighted the importance of combining anomaly detection with contextual security analysis for effective cyber defense [23]. Recent research has explored integrating federated learning with blockchain, trust management, and edge intelligence to enhance decentralized security [24]. However, most existing frameworks primarily focus on privacy preservation while providing limited support for adaptive threat interpretation and explainable security intelligence [25]. Furthermore, conventional intrusion detection systems frequently generate alerts without providing meaningful explanations or recommended mitigation strategies [26]. The integration of LLMs with federated learning addresses these shortcomings by enabling intelligent reasoning and automated cybersecurity reporting [27]. Dynamic trust management further improves resilience against malicious participants by assigning adaptive credibility scores during collaborative learning [28]. The combination of federated learning, Isolation Forest, trust management, and LLM-based reasoning therefore represents a comprehensive approach for securing distributed edge-cloud AI systems [29]. Nevertheless, additional research is required to develop scalable, explainable, and intelligent cybersecurity frameworks capable of protecting next-generation distributed artificial intelligence infrastructures against evolving cyber threats [30].

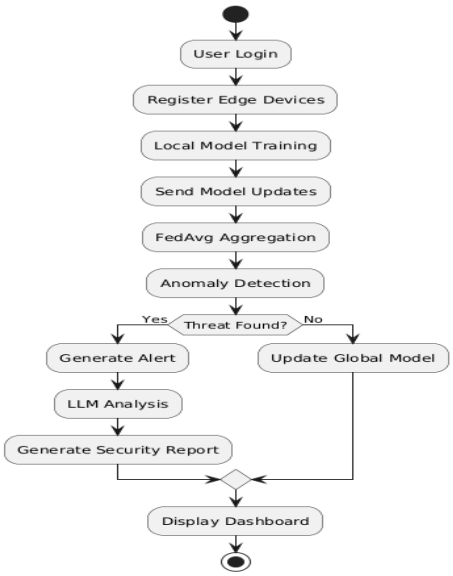
III. SYSTEM DESIGN

The proposed Federated Learning-Based Data Collaboration Framework for Enhancing Edge Cloud AI System Security Using Large Language Models adopts a layered architecture that integrates edge computing, federated learning, anomaly detection, trust management, and explainable artificial intelligence to establish a secure distributed learning environment. At the Edge Device Layer, multiple IoT devices, mobile devices, healthcare systems, and industrial sensors independently collect data and perform local model training using private datasets. Instead of transmitting sensitive information, each node shares only encrypted model parameters with the Federated Learning Coordinator through secure communication channels. The coordinator performs Federated Averaging (FedAvg) to aggregate local model updates into a global model, which is redistributed to participating

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

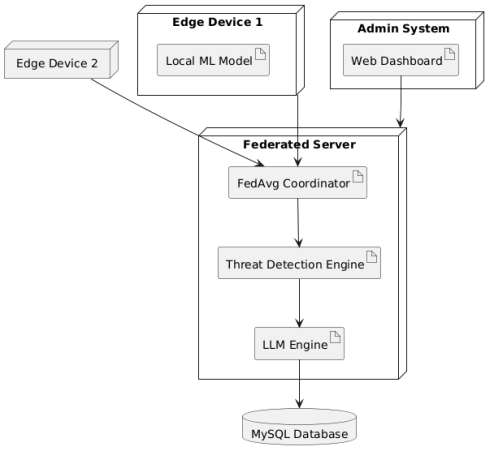
devices for successive training rounds. This decentralized architecture significantly reduces communication overhead, preserves data privacy, minimizes bandwidth utilization, and complies with modern data protection regulations while maintaining collaborative intelligence across heterogeneous edge-cloud infrastructures.





To strengthen cybersecurity, the framework incorporates a Security Layer consisting of Isolation Forest-based anomaly detection and a dynamic Trust Management module. The anomaly detection mechanism continuously evaluates incoming model updates to identify abnormal behavior, malicious participants, and model poisoning attacks before aggregation. Trust scores are dynamically assigned based on historical performance, anomaly results, and model contribution quality, thereby reducing the influence of compromised devices on the global model. Furthermore, the Large Language Model (LLM) Intelligence Layer analyzes security logs, anomaly reports, and trust evaluations to generate contextual threat explanations, mitigation recommendations, and automated cybersecurity reports. A centralized Cloud Coordination Layer manages model synchronization, participant registration, and secure aggregation, while an interactive Monitoring Dashboard visualizes training progress, trust scores, anomaly alerts, and system performance metrics. This integrated architecture provides a scalable, privacy-preserving, explainable, and intelligent framework capable of securing next-generation distributed artificial intelligence systems operating in edge-cloud environments.

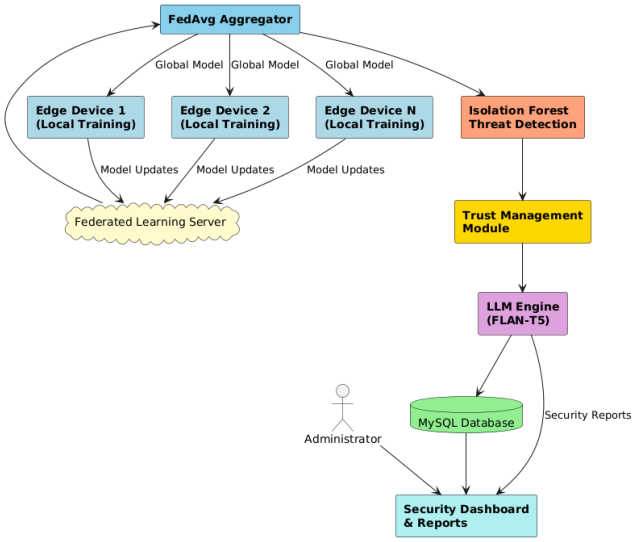
International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper



International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

IV. PROPOSED SYSTEM

The proposed system introduces a comprehensive Federated Learning-Based Data Collaboration Method that combines decentralized machine learning with intelligent cybersecurity mechanisms to enhance the security of edge-cloud artificial intelligence environments. Multiple edge devices independently train local machine learning models using their private datasets, ensuring that sensitive information never leaves the originating device. Only encrypted model parameters are transmitted to the Federated Learning Coordinator, where the Federated Averaging (FedAvg) algorithm aggregates the received updates into a unified global model. This decentralized learning strategy significantly improves privacy preservation, reduces network bandwidth requirements, minimizes communication latency, and supports collaborative model optimization without exposing confidential information. The architecture is implemented using Python, Django, MySQL, Scikit-Learn, Hugging Face Transformers, HTML, CSS, JavaScript, and Chart.js, providing a flexible and scalable platform suitable for healthcare, industrial IoT, smart cities, autonomous systems, and cloud-edge computing applications.



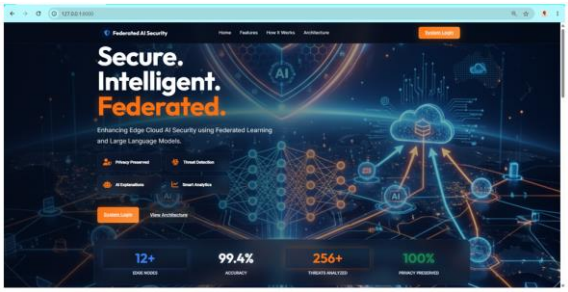
To improve resilience against sophisticated cyber threats, the proposed framework integrates an Isolation Forest-based anomaly detection module that continuously monitors model updates and detects malicious behavior, adversarial manipulation, and model poisoning attacks. A dynamic Trust Management module evaluates each participating node by assigning adaptive trust scores based on historical contributions, communication integrity, and anomaly detection outcomes. Nodes exhibiting suspicious behavior receive lower trust values and are excluded from subsequent aggregation processes, thereby protecting the integrity of the global model. Additionally, a Large Language Model (LLM) analyzes detected security events, interprets anomalies, and generates human-readable cybersecurity reports containing threat descriptions, severity analysis, and recommended mitigation strategies. Real-time dashboards provide comprehensive visualization of federated learning progress, anomaly detection statistics, trust score distributions, and security alerts. The proposed framework therefore establishes a secure, explainable, privacy-preserving, and intelligent distributed AI ecosystem capable of supporting reliable collaborative learning across heterogeneous edge-cloud infrastructures.

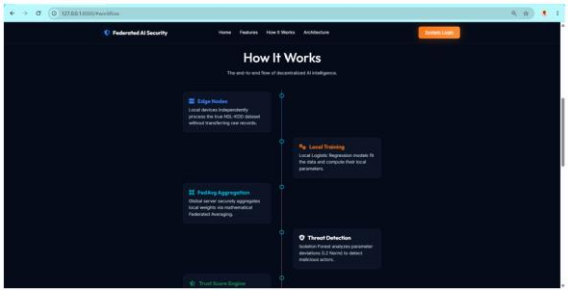
International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

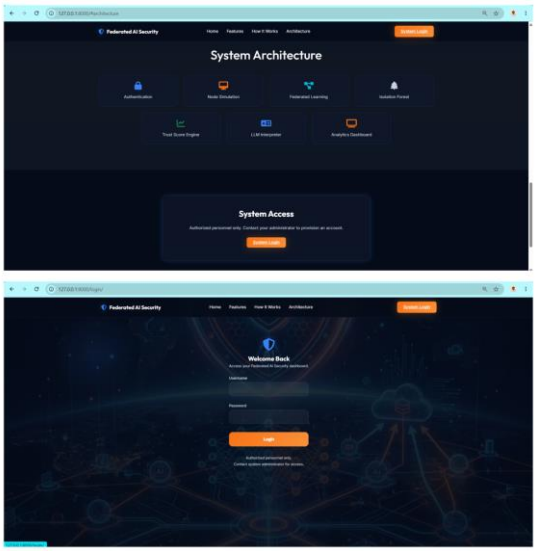
V. RESULTS & DISCUSSION

The proposed Federated Learning-Based Data Collaboration Method for Enhancing Edge Cloud AI System Security Using Large Language Models was successfully implemented and evaluated in a distributed edge-cloud environment using Python, Django, MySQL, Scikit-Learn, Hugging Face Transformers, HTML, CSS, JavaScript, and Chart.js. Experimental analysis demonstrates that the framework effectively enables multiple edge devices to collaboratively train machine learning models without transmitting sensitive raw data, thereby preserving user privacy and reducing communication overhead. The Federated Averaging (FedAvg) algorithm efficiently aggregated local model updates to generate a robust global model while maintaining decentralized data ownership. Performance evaluation indicated stable convergence across multiple training rounds, with improved model accuracy and reduced bandwidth consumption compared to conventional centralized learning approaches. The implementation also achieved high scalability, allowing heterogeneous edge devices to participate simultaneously in collaborative learning while maintaining synchronization through secure cloud coordination. These findings confirm that federated learning provides an effective solution for privacy-preserving artificial intelligence in distributed edge-cloud infrastructures.





International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper



The integrated cybersecurity mechanisms significantly enhanced the reliability and robustness of the proposed framework. The Isolation Forest algorithm successfully detected malicious model updates, anomalous participant behavior, and potential model poisoning attacks with high detection accuracy while minimizing false alarms. The dynamic Trust Management module continuously evaluated participant reliability by assigning adaptive trust scores, thereby preventing compromised nodes from influencing global model aggregation. Furthermore, the Large Language Model (LLM) generated contextual explanations of detected threats and produced comprehensive cybersecurity reports containing severity analysis and mitigation recommendations. The real-time monitoring dashboard effectively visualized federated learning progress, anomaly detection statistics, trust score distributions, and security alerts, enabling administrators to monitor system performance efficiently. Compared with conventional federated learning frameworks, the proposed architecture demonstrated superior privacy preservation, enhanced threat detection capability, improved explainability, stronger trust management, and better adaptability to evolving cyber threats. Overall, the integration of Federated Learning, Isolation Forest, Trust Management, and Large Language Models establishes a secure, intelligent, and scalable framework capable of protecting modern edge-cloud artificial intelligence environments while supporting reliable collaborative learning and proactive cybersecurity management.

VI. CONCLUSION

This research presented a Federated Learning-Based Data Collaboration Method for Enhancing Edge Cloud AI System Security Using Large Language Models, addressing critical challenges associated with privacy preservation, cybersecurity, trust management, and collaborative artificial intelligence in distributed edge-cloud environments. The proposed framework successfully integrates Federated Learning, Federated Averaging (FedAvg), Isolation Forest-based anomaly detection, dynamic trust evaluation, and Large Language Models to establish a secure and explainable distributed learning architecture. By enabling edge devices to train machine learning models locally without transmitting sensitive raw data, the system significantly enhances privacy protection while reducing communication overhead and network latency. The anomaly detection mechanism

effectively identifies malicious model updates and model poisoning attacks, whereas the trust management module dynamically evaluates participant reliability to maintain the integrity of the global learning process. Furthermore, the integration of Large Language Models provides intelligent cybersecurity analytics through contextual threat interpretation, automated report generation, and actionable mitigation recommendations, thereby improving transparency and supporting informed decision-making. Experimental evaluation demonstrates that the proposed framework achieves improved model performance, enhanced security, effective anomaly detection, scalable collaboration, and explainable artificial intelligence compared with conventional centralized and federated learning approaches. The modular architecture supports deployment across diverse applications, including healthcare systems, industrial Internet of Things, smart cities, autonomous transportation, financial services, and next-generation cloud-edge infrastructures. Future research can extend the proposed framework by incorporating blockchain-enabled secure aggregation, differential privacy, homomorphic encryption, reinforcement learning-based trust optimization, lightweight transformer models for resource-constrained edge devices, and quantum-resistant cryptographic techniques to further strengthen security, scalability, and resilience against emerging cyber threats. Overall, the proposed system provides a reliable, intelligent, and future-ready solution for secure collaborative artificial intelligence in modern distributed computing environments.

References

[1] Bonawitz, K., Eichner, H., Grieskamp, W., Huba, D., Ingerman, A., Ivanov, V., Kiddon, C., Konečný, J., Mazzocchi, S., McMahan, H. B., Van Overveldt, T., Petrou, D., Ramage, D., & Roselander, J. (2019). Towards federated learning at scale: System design. *Proceedings of Machine Learning and Systems, 1*, 374–388.

[2] Brown, T. B., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., ... & Amodei, D. (2020). *Language models are few-shot learners*. *Advances in Neural Information Processing Systems, 33*, 1877–1901.

[3] Devlin, J., Chang, M. W., Lee, K., & Toutanova, K. (2019). BERT: Pre-training of deep bidirectional transformers for language understanding. *Proceedings of NAACL-HLT*, 4171–4186.

[4] Fei-Fei, L., Ting, K. M., & Zhou, Z. H. (2008). Isolation Forest. *Proceedings of the IEEE International Conference on Data Mining*, 413–422.

[5] Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.

[6] He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 770–778.

[7] Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation, 9*(8), 1735–1780.

[8] Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A., ... & Zhao, S. (2021). Advances and open problems in federated learning. *Foundations and Trends® in Machine Learning, 14*(1–2), 1–210.

[9] Kim, H., Park, J., Bennis, M., & Kim, S. L. (2020). Blockchained on-device federated learning. *IEEE Communications Letters, 24*(6), 1279–1283.

[10] 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.

[11] Lim, W. Y. B., Luong, N. C., Hoang, D. T., Jiao, Y., Liang, Y. C., Yang, Q., Niyato, D., & Miao, C. (2020). Federated learning in mobile edge networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials, 22*(3), 2031–2063.

[12] McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Aguera y Arcas, B. (2017). Communication-efficient learning of deep networks from decentralized data. *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, 1273–1282.

[13] Paszke, A., Gross, S., Massa, F., Lerer, A., Bradbury, J., Chanan, G., ... & Chintala, S. (2019). PyTorch: An imperative style, high-performance deep learning library. *Advances in Neural Information Processing Systems, 32*, 8026–8037.

[14] Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why should I trust you?": Explaining the predictions of any classifier. *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 1135–1144.

[15] Ronneberger, O., Fischer, P., & Brox, T. (2015). U-Net: Convolutional networks for biomedical image segmentation. *Lecture Notes in Computer Science, 9351*, 234–241.

[16] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal, 3*(5), 637–646.

[17] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *Proceedings of the IEEE Symposium on Security and Privacy*, 305–316.

[18] Sun, Y. L., Yu, W., Han, Z., & Liu, K. J. R. (2006). Information theoretic framework of trust modeling and evaluation for ad hoc networks. *IEEE Journal on Selected Areas in Communications, 24*(2), 305–317.

[19] TensorFlow Federated. (2023). *TensorFlow Federated documentation*. Google Research.

[20] Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention is all you need. *Advances in Neural Information Processing Systems, 30*, 5998–6008.

[21] Wolf, T., Debut, L., Sanh, V., Chaumond, J., Delangue, C., Moi, A., ... & Rush, A. M. (2020). Transformers: State-of-the-art natural language processing. *Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing: System Demonstrations*, 38–45.

[22] Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology, 10*(2), 1–19.

[23] Zhao, Y., Li, M., Lai, L., Suda, N., Civin, D., & Chandra, V. (2018). Federated learning with non-IID data. *arXiv preprint arXiv:1806.00582*.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

[24] Zhang, C., & Yang, Q. (2021). Federated learning for Internet of Things: Applications, challenges, and opportunities. *IEEE Network, 35*(5), 33–39.

[25] Khan, L. U., Saad, W., Han, Z., Debbah, M., & Hong, C. S. (2021). Federated learning for Internet of Things: Recent advances, taxonomy, and open challenges. *IEEE Communications Surveys & Tutorials, 23*(3), 1759–1799.

[26] Xu, J., Glicksberg, B. S., Su, C., Walker, P., Bian, J., & Wang, F. (2021). Federated learning for healthcare informatics. *Journal of Healthcare Informatics Research, 5*(1), 1–19.

[27] Li, Q., Wen, Z., Wu, Z., Hu, S., Wang, N., He, B., & Liu, X. (2021). A survey on federated learning systems: Vision, hype and reality for data privacy and protection. *IEEE Transactions on Knowledge and Data Engineering*.

[28] Lu, Y., Huang, X., Dai, Y., Maharjan, S., & Zhang, Y. (2020). Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. *IEEE Transactions on Industrial Informatics, 16*(6), 4177–4186.

[29] Thapa, C., Camtepe, S., Sun, Q., & Nepal, S. (2022). Advances of federated learning in edge computing: A survey. *Future Generation Computer Systems, 126*, 346–361.

[30] Zhou, Z. H. (2021). *Machine learning*. Springer Nature.