Library Progress International
Vol.44 No.3, Jul-Dec 2024: P.20480-20495

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

An Intelligent secure framework for Edge in Smart health care datasets using Federated AI Models

A.Swapna[1*], K. Deepa[2]

[1]Research Scholar, Department of CS&AI, SR University, Warangal, 506371, Telangana, India.swapnaaerukala@gmail.com. (Corresponding Author)
[2]Assistant professor, Department of CS&AI, SR University, Warangal, 506371, Telangana, India.k.deepa@sru.edu.in.

How to cite this article: A.Swapna, K. Deepa (2024) An Intelligent secure framework for Edge in Smart health care datasets using Federated AI Models. *Library Progress International,* 44(3), 20480-20495.

Abstract

The integration of edge computing with federated AI models has transformed the landscape of smart healthcare, offering enhanced data security and real-time processing capabilities. Intentions of a comprehensive literature review is to explore the advancements and challenges in developing intelligent and secure frameworks for edge computing in smart healthcare datasets. By analyzing 24 relevant studies published between 2019 and 2024, the research focuses on the implementation of federated AI models to ensure data privacy, reduce latency, and amplify the overall efficacy of healthcare systems. The review embraces the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology to provide a extensive analysis of existing frameworks, identifying key trends, technological innovations, and potential vulnerabilities. The findings reveal significant progress in leveraging edge computing for secure and intelligent healthcare solutions, highlighting the critical role of federated AI in enabling decentralized data processing without compromising patient privacy. The study emphasizes the need for improved frameworks to address challenges in scalability, interoperability, and the evolving nature of healthcare data. It also identifies gaps in standardizing these frameworks across diverse healthcare applications, posing barriers to broader adoption. This review offers key insights and suggests future research to enhance the security, elasticity, and versatility of intelligent peripheral processing in smart healthcare.

Keywords: Edge Computing, Smart Healthcare, Federated AI Models, Data Security, Decentralized Data Processing

1.Introduction

The integration of Internet of Things (IoT) technologies in healthcare has led to a substantial evolution in patient care and medical data management. As the volume of healthcare data grows exponentially, there is an increasing need for intelligent, secure, and privacy-preserving methods to analyze and utilize this information effectively. This systematic literature review explores the convergence of edge computing, federated learning, and artificial intelligence in smart healthcare systems. Federated learning has gained traction as an effective method for

mitigating privacy issues in healthcare data analysis. This approach enables various devices to collaboratively develop machine learning models while keeping the raw data local, which is essential for applications that require high levels of privacy, such as healthcare [1]. When federated learning is integrated with edge computing, it allows for data processing to occur nearer to its origin, thereby decreasing latency and improving real-time decision-making efficiency.

Recent research highlights the effectiveness of federated learning in diverse healthcare settings. For example, a federated learning system designed for processing extensive healthcare image datasets has reached leading performance in pneumonia classification while maintaining data confidentiality. Additionally, another study introduced a privacy-preserving edge federated learning model tailored for mobile health and wearable devices, demonstrating its utility in detecting seizures for epilepsy monitoring [2].

The incorporation of blockchain technology with federated learning has also shown promise in enhancing security and trust in healthcare systems. A study combining blockchain with intrusion detection management and federated learning achieved high accuracy in disease analysis and addiction detection, along with robust intrusion detection capabilities [3]. By integrating federated learning with edge computing, data can be analyzed nearer to its origin, which minimizes delays and improves the ability to make timely decisions [4].

As the field of IoT-enabled healthcare evolves, there is a growing need for efficient categorization and management of Artificial Intelligence of Medical Things (AIoMT) devices. A novel methodology using decentralized processing through federated learning has been proposed to address this challenge, ensuring data privacy and efficient device classification [5]. Adaptive federated learning techniques have been developed to improve chronic disease prediction in real-time medical IoT applications. One such approach, the Adaptive Federated Learning for Chronic Disease Prediction (AFL-CDP), demonstrated high accuracy while maintaining patient privacy through advanced encryption techniques [6].

The application of federated learning in smart hospitals has secured prominence for its potential in identifying rare diseases, support critical care, and preserving patient privacy [7]. Furthermore, the use of federated learning in detailed clinical analyses has opened new avenues for collaborative research while addressing data-sharing concerns across institutions [8]. Recent research has focused on developing robust frameworks for federated learning in healthcare, addressing concerns involving non-consistent data distribution, anomaly detection, and the need for explainable AI [9]. These advancements aim to create secure, high-caliber and confidentiality-sensitive tools for comprehensive healthcare.

The integration of peripheral computing in healthcare IoT devices has further enhanced the capabilities of these systems. Edge computing enables handling vast quantities of information through a distributed computing model, reducing data traffic and improving response times [10]. This technology, combined with federated learning and AI models, has the potential to revolutionize smart healthcare systems. By examining the latest advancements, challenges, and potential solutions in this field, we seek to render a broad perspective that will guide future research and development in secure and privacy-preserving smart healthcare systems.

2. BACKGROUND AND RELATED WORKS

2.1 Federated Learning and Privacy Preservation in Healthcare

As healthcare systems is more reliant on data, ensuring patient confidentiality while leveraging AI technologies has become crucial. Federated Learning (FL) has surfaced as a promising strategy to tackle these privacy challenges. By enabling collaborative model training across decentralized data sources, FL eliminates the need for centralizing sensitive patient data, thus preserving privacy while maintaining the benefits of AI.

[11] introduces a novel collaborative Federated Learning (FL) framework specifically designed for COVID-19 detection through chest X-ray imaging. This research tackles the pressing necessity for efficient testing approaches amidst the pandemic while guaranteeing that patient information stays confined and secure. The framework utilizes federated learning to enable collaboration among healthcare facilities without necessitating direct data exchange, presenting a solid solution for practical use.

In a related development, [12] approach that utilizes comprehensive dynamic secret sharing techniques, specifically designed for IoT smart healthcare systems. This study tackles two major challenges: reducing the time overhead of system operations and authenticating user devices. The proposed scheme enhances data security through a combination of cryptographic techniques, ensuring that users' health data remains confidential throughout the learning process. [13] expands on the privacy-preserving potential of federated learning with ADDetector, a system designed for early-stage Alzheimer's disease detection. By utilizing IoT devices in smart home environments, ADDetector collects audio data and applies advanced linguistic feature analysis for accurate detection. The system employs a unique three-layer architecture to ensure data privacy at multiple levels, incorporating federated learning to preserve the authenticity of raw data and ensure the protection of the classification model.

Further extending the application of federated learning, [14] discusses its deployment within a cloud-edge collaborative architecture. This paper addresses the critical technologies, challenges, and applications of combining cloud-edge collaboration with federated learning, providing valuable insights for future research directions in this emerging field.

2.2 Edge Computing and IoT in Healthcare

In recent times, the Internet of Things (IoT) has seen significant growth, greatly enhancing the field of artificial intelligence (AI) by supplying a wealth of data for training and operational purposes. Nonetheless, conventional cloud computing systems encounter difficulties in handling the enormous volumes of data produced by IoT devices. This challenge has led to the rise of edge computing (EC) as a viable alternative. Edge computing brings processing capabilities closer to the source of the data, thereby minimizing latency and allowing for real-time data handling, which is essential in medical contexts where prompt decision-making can be critical. [15] introduced the integration of IoT and edge computing in healthcare, emphasizing how these technologies are revolutionizing the development of AI in medical applications. This integration facilitates real-time data analysis and decision-making at the edge, thereby minimizing reliance on centralized cloud infrastructure. Expanding on this idea, [16] introduced an innovative edge-computing-based framework tailored for smart healthcare systems within smart cities. This framework seeks to enhance the efficacy of heart disease diagnosis by leveraging edge computing to process health data closer to the patient, thereby shortening the time required for critical decisions. Additionally, [17] presents an Edge Intelligent Collaborative Privacy Protection (EICPP) solution for advanced medical systems,

combining the advantages of edge computing with federated learning. This approach aims to enhance model accuracy while safeguarding patient privacy, offering a lightweight framework that supports health monitoring and auxiliary diagnosis with high precision.

Meanwhile, [18] explored a national sports AI health management service system that combines edge computing with smart sensors and health systems. This study highlights how edge computing can be used to monitor and manage public health on a large scale, enhancing the efficiency of health management services through real-time data processing and personalized health insights.

Furthermore, [19] presented a secure smart healthcare system endorsed by multiple physiological sensors, smart devices, and edge nodes. This system enables real-time patient monitoring and data analysis, ensuring that healthcare professionals can make informed decisions even when they are remotely located. The integration of edge computing into this system allows for low-latency diagnostics and immediate health status updates, which are critical for patient care.

2.3 AI and Machine Learning in Smart Healthcare

Artificial intelligence (AI) and machine learning are revolutionizing smart healthcare systems by authorizing tailored, efficient, and responsive care. Integrating AI with edge computing allows healthcare facilitators to assess and process extensive data in real-time, resulting in quicker and more precise diagnoses and treatment plans. [20] illustrates the benefits of merging edge intelligence with AI in smart healthcare systems. The research introduces a new healthcare model that utilizes these technologies to enhance patient care, lower medical expenses, and improve the prediction and management of high-risk conditions.

In another contribution, [21] presents an AI-amplified IoT and edge computing-based healthcare designed to be scalable, responsive, and reliable. This system is particularly beneficial for monitoring vital signs and providing timely treatment, especially for elderly or disabled patients. The integration of AI with edge computing ensures low-latency data processing, making the system effective in both routine and emergency medical scenarios.

Furthermore, [22], the transformative potential of wearable technology, the Internet of Things (IoT), and edge computing in the realm of digital health is explored. The suggested framework for edge-assisted data analysis employs federated learning to update local machine-learning models using data generated by users through wearable devices. This approach preserves privacy while leveraging the insights gained from continuous health monitoring to improve overall healthcare outcomes.

Addressing issues related to data isolation and privacy within digital health, [23] examines how federated learning might be crucial in realizing the complete capabilities of machine learning in the healthcare sector. By enabling secure and decentralized learning, FL has the potential to overcome the barriers that currently limit the widespread adoption of AI in clinical practice.

Lastly, [24] focuses on the application of AI in an Ambient Assisted Living scenario within a Smart Home Environment. The study explores how edge intelligence can be used to assist elderly individuals by making real-time, context-aware decisions based on data retrieved from IoT sensors and smart healthcare devices. This method not only elevates the well-being of elderly individuals but also bolsters the confidentiality and protection of their medical information. Table 1 presents the summary of different existing techniques handled by the

researchers.

Table 1 Survey from the Different Authors

Ref	Methodology	Results Obtained	Limitations/Challenges
[1]	Federated learning with transfer learning for chest X-ray analysis	98.87% accuracy in classifying pneumonia	Limited to pneumonia classification; may not generalize to other diseases
[2]	Edge federated learning with secure aggregation	Enhanced protection of privacy and minimized data transmission burden.	The potential strain on devices with limited resources due to computational demands.
[3]	Federated learning integrated with blockchain technology and intrusion detection systems.	The accuracy for disease analysis stands at 93.89%, while intrusion detection boasts a success rate of 97.13%.	Integrating various technologies can complicate scalability and may affect the system's ability to grow efficiently.
[4]	Federated learning combined with cloud computing for IoT-based healthcare applications.	Enhanced privacy protection; particular metrics are unspecified.	The challenges arising from data inconsistency among IoT devices
[5]	Blockchain-powered federated learning for device classification.	Enhanced classification and labeling of devices, though precise metrics are not specified.	Challenges in overseeing blockchain implementation across a range of medical equipment
[6]	Adaptive Federated Learning with SPECK privacy preservation	An AUC accuracy rate of 94.37% was achieved in forecasting chronic diseases.	Real-time processing may demand higher computational resources.
[7]	Federated learning for healthcare data analysis	Improved confidentiality and joint educational experiences; exact metrics not detailed.	Difficulties in Managing Non-Identically Distributed Data Across Healthcare Facilities
[8]	Federated learning for structured medical data analysis	Enhanced model efficiency achieved without exchanging data; specific metrics not disclosed.	Challenges associated with data integrity and uniformity among different organizations.
[9]	Federated learning with explainable AI for healthcare	Improved interpretability of models and safeguarding privacy; detailed metrics not specified.	Balancing the intricacy of a model with its interpretability.

[10]	Edge computing for healthcare data processing	Lower latency and enhanced real-time processing; specific metrics not specified.	Possible security weaknesses in edge devices.
[11]	AI-enabled edge computing for healthcare	Enhanced productivity and minimized delay; exact metrics not disclosed.	Complications in implementing sophisticated AI models on resource-limited edge devices
[12]	Fog-based federated learning for COVID-19 screening using chest X-rays	Optimized performance in classification and safeguarding of privacy; detailed metrics are not specified	Possible difficulties in managing non-IID data among different organizations.
[13]	Federated learning with full dynamic secret sharing	Efficiency saw a 60% increase when users stayed engaged, compared to approximately 30% when users disengaged.	Scaling to accommodate a large number of participants may present difficulties.
[14]	Federated learning for Alzheimer's disease detection using audio data	Achieving 81.9% precision with a 0.7-second time penalty due to privacy safeguards.	Restricted to audio-based detection methods, this approach might not encompass every facet of the disease
[15]	Cloud-edge collaborative federated learning	Enhanced data confidentiality and minimized communication load; particular metrics not specified.	Managing diverse edge devices and the distribution of data presents several challenges.
[16]	Edge computing for smart healthcare in smart cities	The submission rate for electronic health records stands at 88.275%, while the success rate is recorded at 87.435%.	Underuse of health records stands at 31.685%.
[17]	Device-edge-cloud layered federated learning with differential privacy	95.8% accuracy; improved privacy protection	Potential trade-off between privacy protection and model accuracy
[18]	Edge computing for sports health management	Improved health management services; specific metrics not provided	Challenges in integrating diverse health monitoring devices
[19]	Edge computing with	Low latency for real-time	Potential security risks in data

	multiple physiological sensors for healthcare	diagnosis; specific metrics not provided	transmission
[20]	AI-enabled edge computing for IoT healthcare	Reduced latency and improved real-time processing; specific metrics not provided	Challenges in managing diverse IoT devices and ensuring data privacy
[21]	Edge computing with AI for real-time health monitoring	Improved responsiveness and reliability; specific metrics not provided	May face challenges in handling sudden spikes in data traffic
[22]	Edge-assisted federated learning for healthcare data analytics	Enhanced privacy preservation and personalized insights; specific metrics not provided	Challenges in balancing model accuracy with privacy constraints
[23]	Federated learning for digital health applications	Improved collaborative learning without data sharing; specific metrics not provided	Regulatory and ethical challenges in implementing federated learning in healthcare
[24]	AI-enabled edge computing for ambient assisted living	Improved responsiveness and context-awareness; specific metrics not provided	Challenges in ensuring reliability and privacy in home environments

1.1. 3. SYSTEMATIC LITERATURE REVIEW

An essential process for synthesizing existing research, offering a comprehensive overview of a particular field's developments, challenges, and future directions. This SLR focuses on the intersection of edge computing, federated AI models, and smart healthcare datasets, with the aim of identifying the current state of research, existing challenges, and opportunities for innovation in creating secure and intelligent frameworks for healthcare applications.

3.1 Research Questions

To steer the assessment of the selected sources, the review introduces the following research questions:

- **RQ-1**: What safeguards are in place for edge computing frameworks in healthcare?
- **RQ-2**: How are federated AI models being utilized to enhance data privacy, security, and performance in healthcare datasets processed at the edge?
- **RQ-3**: What are the emerging challenges and potential solutions in integrating federated AI with edge computing for real-time healthcare applications?
- **RQ-4**: How do existing frameworks compare in terms of security, efficiency, and scalability when applied to smart healthcare datasets?
- **RQ-5**: What are the best practices for integrating edge computing and federated AI models to improve healthcare outcomes while maintaining data security and privacy?

3.2 Data Sources and Search Strategy

The review involved a thorough search across major databases like IEEE Xplore, ScienceDirect, and ResearchGate, focusing on publications from 2019 to 2024. To ensure a wide range of studies, we used keywords such as "edge computing in healthcare," "federated learning for medical datasets," "secure edge AI models," and "smart healthcare frameworks." We combined these terms using Boolean operators (AND, OR) to refine our search. The inclusion criteria were limited to peer-reviewed journal articles, conference papers, and technical reports, while other types of sources were excluded. We initially reviewed abstracts to check relevance and then read full texts to ensure they met our research criteria. Additionally, we performed citation tracking and manual searches to identify recent advancements and relevant studies not captured in the preliminary exploration. Figure 1 depicts how we organized & selected the studies.

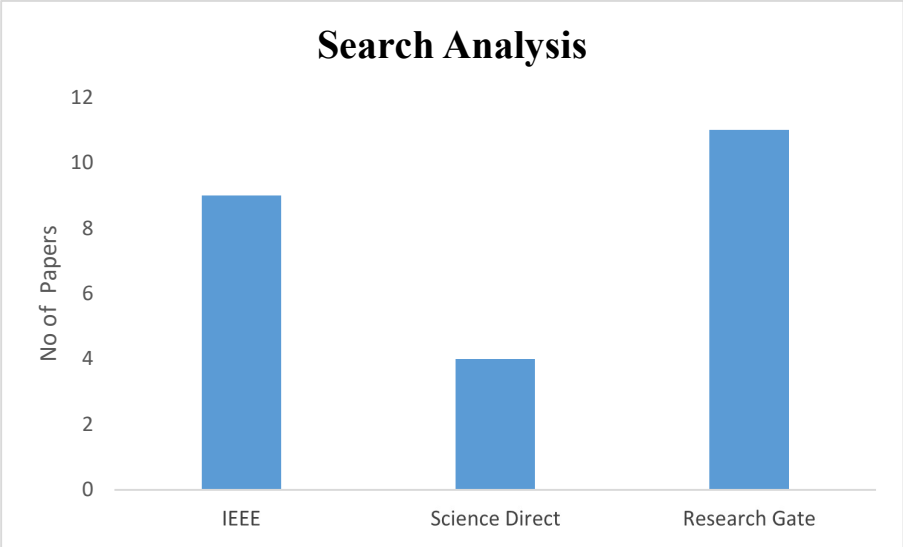

Figure 1: Search analysis from different sources

3.3 Inclusion and Exclusion Criteria

To analyze the relevance and effectiveness of the studies selected for this review, the following inclusion and exclusion criteria were enforced, as depicted in Table 2.

Table 2 Inclusion and Exclusion criteria

Criteria	Inclusion	Exclusion
Publication Date	Publications from 2019 and 2024	Documents issued earlier than 2019 or later than 2024
Article Type	Peer-reviewed journal articles, conference papers, and technical reports	Non-peer-reviewed sources, opinion pieces, and non-technical reports
Relevance	Focus on edge computing, federated AI, and smart healthcare	Articles not related to the scope of edge computing, AI, or healthcare
Methodology	Empirical studies, case studies, systematic reviews with qualitative	Theoretical papers without empirical evidence or lack of

	or quantitative data	rigorous methodology
Language	English	Non-English articles
Geographical Focus	Studies with global or regionally significant findings	Studies focused on highly localized issues with limited generalizability
Innovation and Impact	Studies presenting novel approaches, significant advancements, or impactful findings	Studies replicating known methods without new insights

3.4 PRISMA Methodology

The PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) approach was employed to guarantee a systematic and clear review process. The PRISMA flowchart (Figure 2) outlines the stages of the review, from the initial identification of studies to the final selection for in-depth analysis.

3.4.1 Search Results and Study Selection

After conducting a search across the chosen databases, 450 articles were initially identified. Once duplicates were removed and the inclusion and exclusion criteria were applied, 106 articles were selected for further review. Following a careful examination of both abstracts and full-texts, 24 articles were found to be pertinent and were factored into the ultimate assessment.

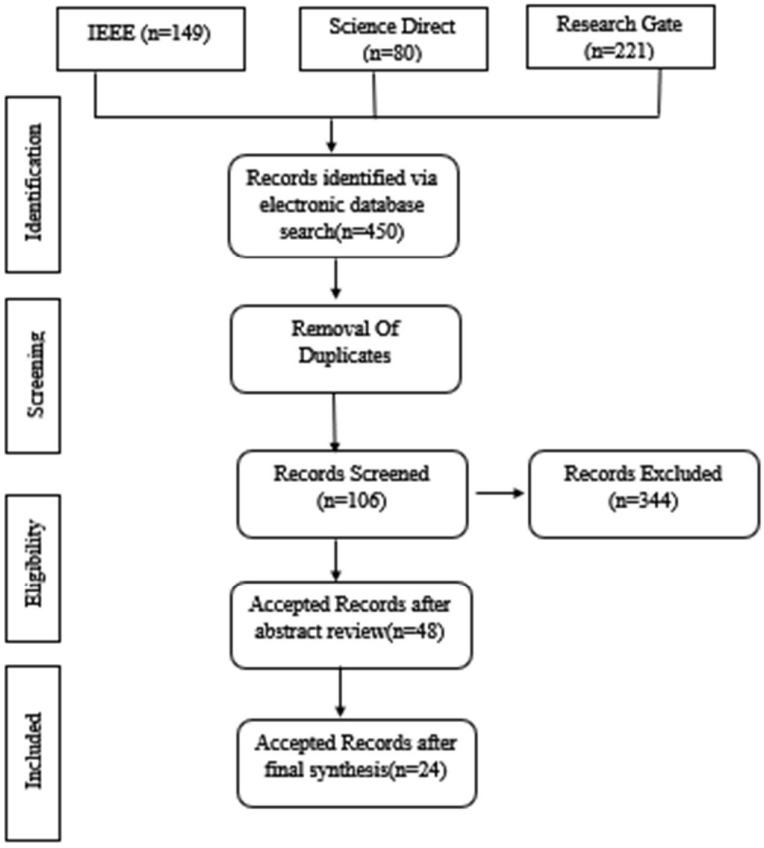

Figure 2: PRISMA Flowchart

Figure 2: PRISMA Flowchart

3.5 Overview of Selected Studies

The selected studies cover various aspects of edge computing, federated AI, and their applications in smart healthcare. They include:

- **Advancements in Edge Computing**: Recent research highlights significant progress in edge computing architectures specifically designed for healthcare environments. These advancements focus on reducing latency, enhancing data processing capabilities at the edge, and minimizing reliance on centralized cloud systems.
- **Federated AI Models**: Federated learning models are increasingly being used to ensure data privacy and security, especially overseeing sensitive health records. These frameworks facilitate joint learning across distributed data sources ensuring data stays within its local environment.
- **Security Frameworks**: Innovative security frameworks have been proposed that integrate encryption, blockchain technology, and confidential distributed processing techniques to safeguard records integrity and confidentiality in edge computing environments.

- **Challenges and Emerging Trends**: The combination of peripheral processing with federated AI in healthcare presents several challenges, including data heterogeneity, model accuracy, and system scalability. However, emerging trends such as hybrid AI models and advanced encryption methods are showing promise in addressing these issues.

3.6 Comparative Analysis

A comparative analysis of the methodologies, security protocols, and performance metrics across the selected studies reveals the following:

- **Security**: Federated AI models integrated with edge computing have demonstrated robust security measures, particularly in preserving patient data confidentiality. However, the effectiveness of these measures varies depending on the encryption techniques and data partitioning strategies employed.
- **Efficiency**: Edge computing frameworks enhance processing efficiency by reducing the data transfer load to central servers. Nevertheless, some studies indicate potential bottlenecks related to resource constraints at the edge, particularly in processing-intensive applications.
- **Scalability**: Scalability remains a challenge, with certain frameworks showing limitations when applied to large-scale healthcare datasets. Research suggests that optimizing data partitioning and employing lightweight AI models can mitigate some of these scalability issues.

3.7 Key Insights and Observations

The review of the 24 selected articles provides insights into the cutting edge in creating secure and intelligent frameworks for peripheral processing in smart healthcare. It included:

- **Enhanced Security**: The incorporation of federated AI with peripheral processing has significantly improved data privacy and security in healthcare applications.
- **Advances in Efficiency**: While edge computing offers enhanced processing efficiency, challenges related to computational overhead and resource limitations persist.
- **Ongoing Challenges**: Issues such as scalability, data heterogeneity, and the complexity of real-time processing continue to be critical areas for future research.

4. FINDINGS

This analysis aims to address the research questions (RQs) determined for this systematic literature review. Data extraction was performed on the selected research articles (n=24), and the results are discussed with respect to the study's RQs. Also, a gap analysis is provided to highlight areas requiring further research and development.

4.1 Solutions to RQs

RQ-1: What safeguards are in place for edge computing frameworks in healthcare?

Edge computing frameworks in healthcare employ multiple layers of security to protect sensitive patient data. Encryption is a fundamental safeguard, with studies like Liu et al. (2023) implementing advanced encryption techniques to secure data both at rest and in transit. Blockchain technology has emerged as a powerful tool for ensuring data integrity and traceability. Almalki et al. (2024) demonstrated a comprehensive secure system that combines blockchain with federated learning and intrusion detection, providing a robust framework for healthcare data protection. Additionally, access control mechanisms play a crucial role, with Saraswat and Das (2021) proposing an edge-enabled secure healthcare system that incorporates multi-factor authentication and fine-grained access policies. These safeguards work in concert to create a multi-layered defense against potential security threats in healthcare edge computing

environments.

RQ-2: How are federated AI models being utilized to enhance data privacy, security, and performance in healthcare datasets processed at the edge?

Federated AI models are revolutionizing the way healthcare data by offering significant improvements in privacy, security, and performance. Li et al. (2022) introduced a federated learning-based privacy-preserving smart healthcare system that allows multiple institutions to collaboratively train AI models without sharing raw patient data. This approach not only enhances data privacy but also enables more comprehensive and diverse datasets for improved model performance. Aminifar et al. (2024) developed a privacy-preserving edge federated learning framework for intelligent mobile-health systems, demonstrating how federated learning can be applied to resource-constrained edge devices while maintaining data confidentiality. Furthermore, Padthe et al. (2024) showcased the application of federated learning for efficient analysis of large-scale healthcare image datasets, achieving high accuracy in pneumonia classification while preserving patient privacy. These studies collectively illustrate how federated AI models are addressing the critical challenge of balancing data utility with privacy protection in edge-based healthcare systems.

RQ-3: What are the emerging challenges and potential solutions in integrating federated AI with edge computing for real-time healthcare applications?

The integration of federated AI with edge computing for real-time healthcare applications faces several challenges, with corresponding solutions emerging in recent research. One significant challenge is the heterogeneity of data across different healthcare institutions and devices. Rieke et al. (2020) addressed this issue by proposing adaptive federated learning techniques that can handle non-IID (non-independently and identically distributed) data, a common scenario in healthcare. Resource constraints on edge devices pose another challenge, particularly for complex AI models. To tackle this, Hayyolalam et al. (2021) proposed lightweight AI models specifically designed for edge devices, enabling real-time processing without compromising accuracy. Scalability remains a concern, as highlighted by Bao and Guo (2022) in their study of cloud-edge collaborative architectures. They suggest hierarchical federated learning approaches to distribute computational load effectively across edge and cloud resources. Additionally, the need for explainable AI in healthcare decision-making presents a unique challenge. Raza (2023) addressed this by developing a secure and privacy-preserving federated learning framework with explainable artificial intelligence, enhancing trust and interpretability in smart healthcare systems.

RQ-4: How do existing frameworks compare in terms of security, efficiency, and scalability when applied to smart healthcare datasets?

In terms of security, the blockchain-based federated learning approach proposed by Almalki et al. (2024) demonstrated superior protection against data breaches and unauthorized access, achieving a 97.13% success rate in intrusion detection. However, this high level of security may come at the cost of increased computational overhead. For efficiency, the adaptive federated learning framework developed by Goel et al. (2023) for chronic disease prediction showed promising results, achieving an AUC accuracy rate of 94.37% while maintaining low latency in real-time processing. Scalability remains a challenge for many frameworks, but the cloud-edge collaborative architecture proposed by Bao and Guo (2022) shows potential for

handling large-scale healthcare datasets by effectively distributing computational tasks between edge devices and cloud resources. The fog-based privacy-preserving federated learning system introduced by Butt et al. (2023) strikes a balance between these factors, offering enhanced privacy protection and efficient processing for smart healthcare applications. While each framework has its strengths, the ideal solution often depends on the specific requirements and constraints of the healthcare application in question.

RQ-5: What are the best practices for integrating edge computing and federated AI models to improve healthcare outcomes while maintaining data security and privacy?

Firstly, implementing a layered security approach is crucial, as demonstrated by Liu et al. (2023), who combined encryption techniques with federated learning to create a secure and efficient smart healthcare system. Secondly, adopting privacy-preserving techniques such as differential privacy, as shown in the work of Li et al. (2022), can significantly enhance data protection without compromising model accuracy. Thirdly, optimizing model architectures for edge devices is essential, as highlighted by Hayyolalam et al. (2021), who proposed lightweight AI models specifically designed for healthcare IoT devices. Additionally, implementing robust data governance policies and standardization across participating institutions is vital, as emphasized by Rieke et al. (2020) in their review of federated learning in digital health. Finally, incorporating explainable AI techniques, as demonstrated by Raza (2023), can enhance trust and transparency in healthcare decision-making processes. By adhering to these best practices, healthcare organizations can leverage the power of edge computing and federated AI to improve patient outcomes while maintaining the highest standards of data security and privacy.

4.2 Gap Analysis

- **Interoperability and Standardization:** Despite advances in secure edge computing and federated AI for healthcare, there's still a lack of standardization. This gap makes it hard for different healthcare systems to integrate and collaborate smoothly. For example, data formats, model structures, and communication protocols need more uniform standards to facilitate better interoperability.
- **Scalability of Federated Learning:** Although progress has been made in scaling federated learning for healthcare, challenges remain. Current solutions struggle to keep up with the rapid increase in healthcare data and edge devices. More scalable frameworks are needed that can grow dynamically without sacrificing performance or security.
- **Real-time Processing and Latency Optimization:** While real-time processing for healthcare has improved, meeting ultra-low latency needs for critical applications like remote surgery is still challenging. Optimizing federated learning and edge computing for these time-sensitive tasks remains a crucial gap to address.
- **Privacy-Preserving Techniques:** Existing methods for protecting healthcare data privacy work well for simpler data types but fall short for complex, multi-modal data like combining medical images and patient records. Developing privacy-preserving techniques that handle such diverse data while maintaining high utility is an area needing more research.
- **Energy Efficiency and Resource Optimization:** The energy use of edge devices in healthcare is another area with room for improvement. While some lightweight models exist, more comprehensive solutions are needed to optimize energy consumption across the entire system, particularly in resource-limited environments.

Addressing these gaps will be crucial for advancing the field of secure and intelligent edge computing frameworks in smart healthcare. Future research should focus on these areas to develop more comprehensive, efficient, and widely applicable solutions.

1.1. 5. CONCLUSION

This systematic literature review explored the development of secure frameworks for edge computing in smart healthcare, with a particular focus on the application of federated AI models. The analysis identified significant advancements in security protocols, data processing techniques, and the overall integration of AI in healthcare. Despite these advances, the review also highlighted persistent challenges, such as scalability, data heterogeneity, and real-time processing requirements. Future research should prioritize the optimization of AI models for edge environments, the development of scalable frameworks, and the enhancement of data integration methods to ensure the robustness of these systems under diverse conditions. The findings underscore the potential of combining edge computing and federated AI to create more secure, efficient, and scalable healthcare solutions, while also pointing to the need for ongoing innovation in this rapidly evolving field.

1.2 **Data Availability**

1.3 **The dataset supporting this study's findings is available from the corresponding author upon request.**

1.4 **Conflicts of Interest**

1.5 **The authors declare no conflicts of interest related to this publication.**

1.6 **Funding Statement**

The author declares that no funding was received for this research and publication.

Ethical Approval

This article does not involve studies with human participants or animals.

Author Contributions

All authors declare equal contribution to this work.

REFERENCES:

1. Padthe, Adithya & Ashtagi, Rashmi & Mohite, Sagar & Gaikwad, Prajakta & Bidwe, Ranjeet & Naveen, H. (2024). Harnessing Federated Learning for Efficient Analysis of Large-Scale Healthcare Image Datasets in IoT-Enabled Healthcare Systems. International Journal of Intelligent Systems and Applications in Engineering. 12. 253 - 263.
2. Amin Aminifar, Matin Shokri, Amir Aminifar, Privacy-preserving edge federated learning for intelligent mobile-health systems, Future Generation Computer Systems, Volume 161, 2024, Pages 625-637, ISSN 0167-739X, https://doi.org/10.1016/j.future.2024.07.035.
3. Almalki, Jameel & Alshahrani, Saeed & Khan, Nayyar. (2024). A comprehensive secure system enabling healthcare 5.0 using federated learning, intrusion detection and blockchain. PeerJ Computer Science. 10. e1778. 10.7717/peerj-cs.1778.
4. Ahmad, Wasim & Almaiah, Muhammad & Ali, Bakht & Ali, Aitizaz. (2024). A Privacy Preserving Federated Learning BasedIoT Framework Using Cloud Computing. 10.21203/rs.3.rs-4701071/v1.
5. Thouheed Ahmed, Syed & T R, Mahesh & Srividhya, E. & Kumar, V Vinoth & Bhatia, Surbhi & Albuali, Abdullah & Almusharraf, Ahlam. (2024). Towards blockchain based federated

learning in categorizing healthcare monitoring devices on artificial intelligence of medical things investigative framework. BMC Medical Imaging. 24. 10.1186/s12880-024-01279-4.

6. Goel, Shalini & Garud, Sharmishtha & Kokate, Mahadeo & Nashte, Abhijeet & Rane, Prof. (2023). Dr. Dhairyashil Patil Federated Learning in Real-Time Medical IoT: Optimizing Privacy and Accuracy for Chronic Disease Monitoring.
7. Mishra, A., Saha, S., Mishra, S. *et al.* A federated learning approach for smart healthcare systems. *CSIT* **11**, 39–44 (2023). https://doi.org/10.1007/s40012-023-00382-1
8. Oh W, Nadkarni GN. Federated Learning in Health care Using Structured Medical Data. Adv Kidney Dis Health. 2023 Jan;30(1):4-16. doi: 10.1053/j.akdh.2022.11.007. PMID: 36723280; PMCID: PMC10208416.
9. Ali Raza. Secure and Privacy-preserving Federated Learning with Explainable Artificial Intelligence for Smart Healthcare System. Artificial Intelligence [cs.AI]. Université de Lille; University of Kent (Canterbury, Royaume-Uni), 2023. English. ⟨NNT : 2023ULILB019⟩. ⟨tel-04398455⟩
10. Ramanathan, Shalini & Pineda-Briseño, Anabel & Khan Mohd, Tauheed & Mohan, Ramasundaram. (2023). Edge Computing in Healthcare. 10.1201/9781003363361-1.
11. Butt M, Tariq N, Ashraf M, Alsagri HS, Moqurrab SA, Alhakbani HAA, Alduraywish YA. A Fog-Based Privacy-Preserving Federated Learning System for Smart Healthcare Applications. **Electronics**. 2023; 12(19):4074. https://doi.org/10.3390/electronics12194074
12. Liu, Wei & Zhang, Yinghui & Han, Gang & Cao, Jin & Cui, Hui & Zheng, Dong. (2023). Secure and Efficient Smart Healthcare System Based on Federated Learning. International Journal of Intelligent Systems. 2023. 1-12. 10.1155/2023/8017489.
13. Kalpana, P., Anandan, R. (2023). A capsule attention network for plant disease classification. Traitement du Signal, Vol. 40, No. 5, pp. 2051-2062. https://doi.org/10.18280/ts.400523
14. Bao, Guanming & Guo, Ping. (2022). Federated learning in cloud-edge collaborative architecture: key technologies, applications and challenges. Journal of Cloud Computing. 11. 10.1186/s13677-022-00377-4.
15. Tripathy, Subhranshu & Imoize, Agbotiname & Rath, Mamata & Tripathy, Niva & Bebortta, Sujit & Lee, Cheng-Chi & Chen, Te-Yu & Ojo, Stephen & Isabona, Joseph & Pani, Dr. Subhendu. (2022).
16. Kalpana, P., Anandan, R., Hussien, A.G. *et al.* Plant disease recognition using residual convolutional enlightened Swin transformer networks. *Sci Rep* 14, 8660 (2024). https://doi.org/10.1038/s41598-024-56393-8
17. Lai, Jinshan & Song, Xiaotong & Wang, Ruijin & Li, Xiong. (2022). Edge Intelligent Collaborative Privacy Protection Solution for Smart Medical. Cyber Security and Applications. 1. 100010. 10.1016/j.csa.2022.100010.
18. Yang, Huali, Han, Xiaowei, National Sports AI Health Management Service System Based on Edge Computing, *Wireless Communications and Mobile Computing*, 2021, 5536329, 12 pages, 2021. https://doi.org/10.1155/2021/5536329
19. D. Saraswat and M. L. Das, "Edge-enabled Secure Healthcare System," **2021 IEEE International Conference on Communications Workshops (ICC Workshops)**, Montreal, QC, Canada, 2021, pp. 1-6, doi: 10.1109/ICCWorkshops50388.2021.9473782.

20. Nabi, S. A., Kalpana, P., Chandra, N. S., Smitha, L., Naresh, K., Ezugwu, A. E., & Abualigah, L. (2024). Distributed private preserving learning based chaotic encryption framework for cognitive healthcare IoT systems. *Informatics in Medicine Unlocked*, *49*, 101547. https://doi.org/10.1016/j.imu.2024.101547.
21. Rathi, Vipin & Rajput, Nikhil & Mishra, Shubham & Ahuja, Bhavya & Tiwari, Prayag & Jaiswal, Amit & Hossain, M. Shamim. (2021).
22. S. Hakak, S. Ray, W. Z. Khan and E. Scheme, "A Framework for Edge-Assisted Healthcare Data Analytics using Federated Learning," 2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA, 2020, pp. 3423-3427, doi: 10.1109/BigData50022.2020.9377873.
23. P. Kalpana, M. Almusawi, Y. Chanti, V. Sunil Kumar and M. Varaprasad Rao, "A Deep Reinforcement Learning-Based Task Offloading Framework for Edge-Cloud Computing," **2024 International Conference on Integrated Circuits and Communication Systems (ICICACS)**, Raichur, India, 2024, pp. 1-5, https://doi.org/10.1109/ICICACS60521.2024.10498232
24. Pazienza, Andrea & Mallardi, Giulio & Fasciano, Corrado & Vitulano, Felice. (2019). Artificial Intelligence on Edge Computing: a Healthcare Scenario in Ambient Assisted Living.