AI-Driven Fog-Edge Computing for IoMT Systems: Architecture and Use Cases

Babar Shah[1], Muhammad Junaid[2], Hamza Rustam[3], Mohammad Habib[4], Sajid Anwar[5]
[1]College of Technological Innovation, Zayed University, Abu Dhabi, UAE
[2]Department of Statistics, Islamia College University, Pakistan
[3]Department of Computer and Software Technology, University of Swat, Pakistan
[4]Department of Computer Science, Govt PG Jahanzeb College, Pakistan
[5]School of Computer Science and Information Technology, IMSciences, Pakistan
babar.shah@zu.ac.ae, 2021-icp-5502.std@icp.edu.pk, hs4647213@gmail.com, muhammadhabib@jc.edu.pk, sajid.anwar@imsciences.edu.pk

Abstract

The Internet of Medical Things (IoMT) transforms healthcare by enabling real-time monitoring, diagnostics, and treatment through interconnected medical devices. However, data security, privacy, and latency remain critical concerns. This paper proposes an AI-driven fog-edge computing architecture designed to enhance the performance, security, and responsiveness of IoMT systems. We first review recent advances in AI-enabled IoMT platforms and highlight their limitations. We then introduce a novel fog-edge model that integrates artificial intelligence to optimize data processing and decision-making at the network edge, reducing latency and improving system reliability. Strategies for strengthening data security within IoMT environments are also presented. Furthermore, we examine real-world use cases demonstrating the effectiveness of AI-powered fog-edge architectures in healthcare, including their role in enabling contactless patient care. Finally, we discuss problem formulations and data acquisition methods and outline future research directions. This study provides a comprehensive framework for advancing secure and efficient IoMT systems using AI at the fog-edge layer.

Introduction

The Internet of Medical Things (IoMT), an extension of the Internet of Things (IoT), transforms healthcare by connecting smart medical devices that collect, share, and analyze patient data in real-time. IoMT enables continuous health tracking and seamless data flow to healthcare providers with wearable sensors, home monitoring systems, and cloud integration. Combined with Artificial Intelligence (AI), this ecosystem improves diagnostic accuracy, supports personalized treatments, and enables proactive care for chronic conditions. By shifting healthcare from reactive to preventive, IoMT enhances patient outcomes, lowers costs, and optimizes clinical workflows (Bisio et al. 2025; Goel and Neduncheliyan 2024).

IoMT has revolutionized healthcare by enabling real-time patient monitoring and remote care. While it improves patient outcomes, it also raises critical latency and data security challenges. Cloud-based IoMT systems often face delays due to the distance between devices and cloud servers—delays that can be life-threatening in emergencies. Additionally, the growing volume of connected devices strains network capacity. Security is another primary concern, as IoMT systems handle sensitive patient data that must comply with regulations like HIPAA and GDPR (Abdulkareem et al. 2019). With healthcare organizations facing frequent data breaches, strengthening security is essential. To address these issues, this research explores the use of AI-based fog and edge computing, which offer the potential to reduce latency and improve data protection, helping IoMT systems overcome the limitations of traditional cloud architectures.

This research aims to create a strong security framework for IoMT systems, focusing on four key objectives: developing a secure encryption system to protect medical data during transmission, enhancing authentication through improved key reliability and multi-factor identification, building an efficient Intrusion Detection System (IDS) to respond to threats in real-time with reduced false alarms, and evaluating the framework's performance in terms of data confidentiality, system integrity, and attack surface to ensure robust security.

This study makes significant contributions to the security of IoMT systems, introducing a cutting-edge whitening method that fortifies data integrity and mitigates unauthorized access through advanced cryptographic techniques. The research also pioneers integrating multifactor authentication and dynamic key management to bolster access control, safeguarding IoMT systems from breaches in open environments. A sophisticated Intrusion Detection System (IDS) is developed, offering real-time threat monitoring with drastically reduced false positives by leveraging anomaly-based and signature-based techniques. The proposed security framework undergoes a thorough evaluation, demonstrating notable improvements in data protection, system resilience, and defense against simulated and real-world cyber threats. Ultimately, the combination of enhanced access control and an intelligent IDS provides an extra layer of security, ensuring comprehensive, adaptive protection for distributed IoMT systems.

This paper is organized as follows: Section 1 introduces the motivation and objectives of the study, focusing on securing IoMT systems and reducing latency—section 2 reviews related literature on AI-based IoMT platforms. Sec-

tion 3 describes the proposed AI-driven fog-edge architecture for IoMT. Section 4 explores strategies for enhancing data security within IoMT systems. Section 5 presents real-world use cases of AI-enabled fog-edge applications in healthcare. Section 6 highlights the use of fog-edge AI for contactless patient care. Section 7 covers problem formulations and data acquisition.

Overview of AI-enabled IoMT Platforms

IoMT platforms are built on a multi-layered architecture that integrates various components to enable the seamless gathering, transfer, storage, processing, and use of health-related data. The use of fog and edge computing in healthcare has attracted significant research attention for its ability to enhance real-time data processing. Fog computing effectively handles big data in smart cities, offering clear advantages in lowering latency and reducing bandwidth usage compared to traditional cloud computing (Aguru et al. 2022). However, they also raised concerns about security challenges and scalability, noting decentralized systems' lack of robust data protection measures. Similarly, the authors in (Alam et al. 2021; A. and Aldossary 2021) reported improved latency and network efficiency with fog computing in healthcare but highlighted ongoing challenges around data integrity and meeting strict regulatory requirements.

Innovative AI-enabled healthcare systems are typically composed of several essential components, including sensors and devices that collect real-time health data; communication modules that ensure secure data transmission over wired or wireless networks; data storage systems that manage sensitive information with encryption, access control, and compliance measures; and data processing units that apply machine learning and AI algorithms for analysis (Akilan et al. 2023). Additionally, these systems include applications and services, such as web and mobile platforms, to provide healthcare professionals with convenient access to patient information (Shah, Junaid, and Habib 2024). To safeguard sensitive health data, robust security and privacy measures are implemented, including end-to-end encryption, secure authentication, and data masking, ensuring the integrity and confidentiality of patient information.

To develop a highly effective IoMT system, modern supervised AI and ML algorithms have emerged as a promising and rapidly growing area of research. This paragraph highlights several key studies closely related to the proposed study. (Kim et al. 2023) explored heart disease prediction using various medical attributes, designing a model that identifies patients at risk of heart disease. They applied algorithms like K-Nearest Neighbors (KNN) and logistic regression (LR), demonstrating that these methods achieve superior prediction accuracy compared to the Naive Bayes model. Similarly, ML-based diagnostic system was developed for heart disease prediction, leveraging seven ML algorithms—three for feature selection and four for cross-validation (Arcas et al. 2024; Otoum, Ridhawi, and Mouftah 2021). Their model was evaluated using multiple performance metrics, including classification accuracy, sensitivity, specificity, Matthews' correlation coefficient, and execution time. Impressively, the system accurately identified individuals with heart disease and analyzed receiver operating characteristic (ROC) curves and the area under the curve (AUC) for all classifiers, highlighting its robustness and predictive power. Recent studies have explored fog, edge, and cloud computing in IoT-based healthcare to improve data handling, reduce latency, and optimize energy use. (Awaisi et al. 2020) showed these technologies help lower latency and bandwidth but face security challenges, while (Zhang et al. 2024; Tai et al. 2022) highlighted integration and scalability issues. Fog computing combined with machine learning to improve healthcare data processing but stressed the need for stronger data protection (Demirel, Bayoumy, and Faruque 2022). Although integration challenges remained, Ghosh and Mukherjee's STROVE model improved data availability during COVID-19 (S. and Mukherjee 2022). Fuzzy data offloading model was proposed in (K. and Das 2022) that reduced energy use but struggled with real-time big data. (Mukherjee et al. 2021) confirmed that fog and edge computing improve healthcare data handling but warned of security risks and integration complexity. (Jain et al. 2021) applied a fog-–edge–cloud model in smart agriculture, achieving better energy use and data transfer, but facing scalability and data security challenges. Finally, (Hrnandez-Jaimes et al. 2023; Zhang, Ouda, and Abu-Rukba 2024) focused on resource scheduling and energy-efficient architectures for real-time health monitoring, showing gains in efficiency but noting performance limits with large datasets.

AI-based Fog-Edge Model for IoMT

The Fog-Edge Computing model presented in this paper leverages AI-driven algorithms to optimize real-time data analysis in IoT applications for the healthcare sector. By integrating fog and edge computing concepts, the model reduces latency and energy consumption while enhancing the processing of critical healthcare data at the point of demand. AI is pivotal in streamlining data handling, enabling more intelligent decision-making at the edge, and minimizing reliance on cloud computing. This architecture capitalizes on the strengths of both fog and edge computing to offer low-latency, secure, and highly available solutions for time-sensitive healthcare applications, ensuring timely and efficient data analysis for improved patient outcomes. The proposed architecture consists of three main layers as shown in Figure 1.

- **Edge Layer:** This layer includes IoT wearables, such as health monitoring devices and smartwatches, which record vital signs (e.g., HR, BP, temperature). While limited in computational capacity, these devices play a crucial role in real-time monitoring and data classification, including feature extraction and anomaly detection, enhanced by AI algorithms.
- **Fog Layer:** Positioned between the edge and cloud, the fog layer consists of local servers or gateways that handle more complex data processing tasks. It performs analytics, data compilation, and anonymization, leveraging AI for efficient data management with minimal latency while ensuring data protection.

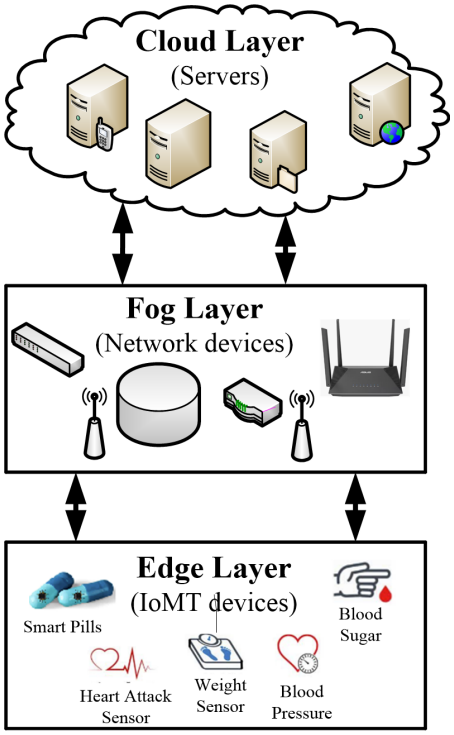

Figure 1: Fog-Edge model for IoMT.

- **Cloud Layer:** The cloud layer stores long-term data and handles advanced analytics, including machine learning model creation and historical data analysis. It focuses on non-real-time computations, complementing the real-time processing done by the edge and fog layers.

The proposed framework optimizes various factors, including bandwidth consumption, task management, and communication overhead, providing a comprehensive view of performance metrics such as latency, energy usage, and data handling across different layers. Total energy consumption is calculated by aggregating the energy used during task execution in the edge and fog layers. The data offloading ratio indicates the proportion of data transferred from the edge to the fog layer, emphasizing maximizing bandwidth utilization while minimizing latency and energy consumption. The objective function balances resource costs with the revenue generated from product sales. Communication overhead, representing the extra time needed to transmit data between layers, is minimized to reduce overall system latency. Additionally, computation distribution between the edge and fog layers is optimized based on processing capabilities and available bandwidth.

Based on the computational capabilities of edge devices, the data collected at the edge layer can be processed locally. Depending on the processing results and the device resources, some data is offloaded to the fog layer for further analysis. The fog layer then handles these tasks and returns the processed information either to the edge layer for real-time feedback or to the cloud for long-term storage and more in-depth analysis. Serving as an intermediary, the fog layer bridges the gap between the edge's real-time processing and the more powerful, but distant, cloud layer. This structure enhances efficiency, reducing latency while ensuring that data is processed and stored optimally.

Enhancing Data Security in IoMT Systems

Securing data in IoMT systems is crucial, given the sensitive nature of healthcare data and the vulnerabilities inherent in interconnected medical devices. To enhance security, various strategies can be employed, taking advantage of AI and advanced technologies, as shown in Figure 2:

- **AI-Powered Threat Detection:** AI and machine learning algorithms can continuously monitor IoMT networks to detect anomalies or potential threats in real time. Through Intrusion Detection Systems (IDS), AI can identify patterns indicative of security breaches, allowing immediate responses to mitigate damage. In addition, AI can predict vulnerabilities by analyzing historical attack data, enabling proactive measures to protect against future breaches.
- **Encryption:** Robust encryption techniques, such as AES and RSA, ensure that patient data remains secure during storage and transmission. AI can assist in enhancing encryption protocols by optimizing key management and identifying potential weaknesses in the encryption process, providing stronger protection against unauthorized access.
- **Authentication and Authorization:** Implementing Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC) ensures that only authorized individuals can access sensitive data. AI can further bolster these systems using biometric data and behavioral analysis for adaptive real-time authentication, providing more secure access control.
- **Data Anonymization:** AI can automate anonymization of Personally Identifiable Information (PII), ensuring that patient data are protected during sharing or processing. By scrubbing sensitive data, AI enhances privacy without compromising the integrity of the dataset.
- **Blockchain Technology:** Blockchain offers a decentralized immutable ledger to record data transactions. AI can be integrated with blockchain to monitor and validate data transactions, automatically detecting real-time discrepancies or unauthorized manipulations.
- **Regular Updates and Compliance:** AI can streamline the process of system updates by automating firmware and software patches as soon as vulnerabilities are detected. In addition, AI-driven tools can perform continuous security audits, ensuring that IoMT systems comply with healthcare regulations such as HIPAA and GDPR.
- **Data Integrity Protocols:** AI can assist in implementing hashing techniques, such as SHA-256, ensuring the integrity of healthcare data. By creating digital fingerprints, AI can detect tampering or unauthorized alterations, preserving the accuracy and trustworthiness of medical information.

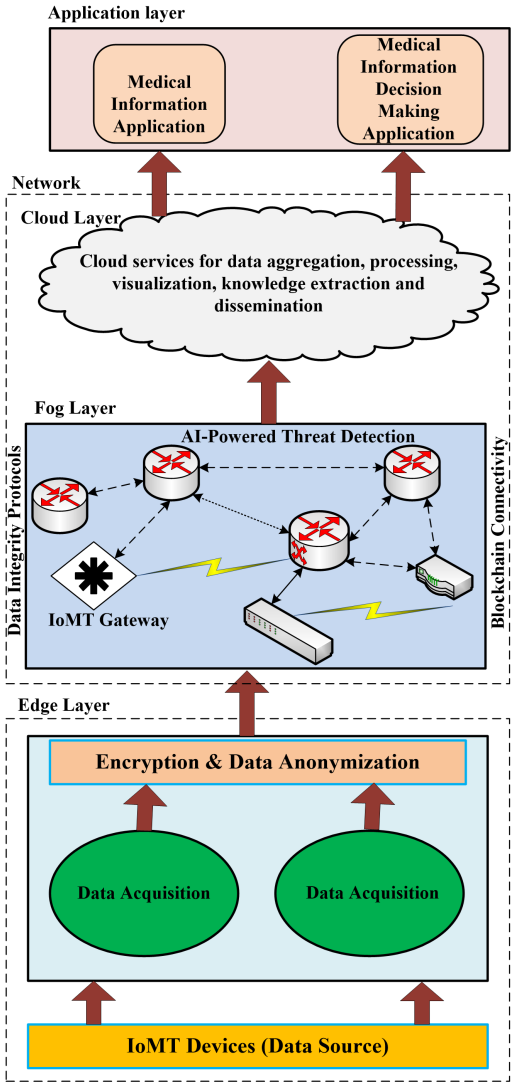

Figure 2: security in IoMT systems.

By combining AI with encryption, authentication, blockchain, and other security measures, IoMT systems can offer enhanced protection of patient data, ensuring its confidentiality, integrity, and availability in the face of growing cyber threats.

Real-World Use Cases of AI-Enabled Fog-Edge Architecture for IoMT

This section provides deeper insights into specific use cases of cutting-edge AI-enabled fog-edge architectures for IoMT platforms.

- **Real-Time Patient Monitoring Emergency Alerts:** In today's connected healthcare landscape, AI at the edge layer enables continuous, intelligent monitoring of patient vitals such as heart rate, blood pressure, and oxygen saturation from wearable devices like smartwatches, fitness trackers, and medical sensors. This allows the system to instantly detect anomalies — for example, identifying signs of arrhythmia, strokes, or sudden oxygen drops in patients with chronic conditions. When critical patterns are detected, the system automatically alerts doctors, nurses, or caregivers, enabling life-saving interventions before the patient reaches a hospital. Meanwhile, the fog layer aggregates and filters data from thousands of devices across a hospital or care network, providing clinicians with a holistic view of patient populations and supporting coordinated responses during emergencies, such as mass casualty events.
- **Predictive Maintenance of Medical Devices:** In modern hospitals, ensuring the continuous availability of critical medical equipment like infusion pumps, ventilators, dialysis machines, and patient monitors is a matter of life and death. With AI-driven fog nodes monitoring the health and performance of these IoMT devices in real-time, hospitals can detect early warning signs, such as abnormal vibration patterns, overheating, or repeated system errors. By analyzing device usage trends and error logs, the system predicts when equipment will likely fail, allowing biomedical engineers to schedule proactive maintenance. This minimizes costly downtime, reduces emergency repairs, and, most importantly, ensures that life-saving devices are always available when patients need them most. This approach has helped hospitals improve operational efficiency, cut maintenance costs, and dramatically improve patient safety outcomes.
- **Personalized Treatment Recommendations:** In today's fast-paced clinical environments, personalized care can differentiate between routine recovery and life-threatening complications. With AI deployed at the edge, real-time patient data, such as blood glucose levels, heart rhythms, or medication adherence, is analyzed directly on wearable or bedside devices. Simultaneously, fog-level models integrate historical records and patterns from multiple patients, enabling richer, context-aware insights. For example, an AI-driven insulin pump can instantly adjust dosing in diabetic patients based on real-time glucose readings and lifestyle data. At the same time, the fog layer refines recommendations using broader patient population trends. This dual-layer system ensures that treatment plans adapt dynamically to each patient's unique needs without delays from cloud processing. In real-world applications, this has improved medication accuracy, reduced hospital readmissions, and improved patient satisfaction, empowering clinicians to deliver precision medicine at the bedside or even at home.
- **Secure Compliant Health Data Sharing:** In an era of connected healthcare, securely exchanging patient data between hospitals, labs, and specialists is critical, but it comes with high stakes. AI-driven fog nodes play a vital role by automatically encrypting and anonymizing patient records before they leave the local network, ensuring that the data remains unintelligible even if intercepted. Advanced authentication mechanisms, like biometric access or multifactor verification, confirm

that only authorized parties can access sensitive health records. To take it further, blockchain and smart contracts can be layered to create a tamper-proof audit trail, guaranteeing compliance with strict regulations like HIPAA or GDPR. For example, when a trauma patient is transferred between hospitals, the system securely shares real-time medical history, imaging, and lab results, ensuring seamless care continuity without risking privacy breaches. This not only builds patient trust but also accelerates treatment decisions, reduces duplication of tests, and improves coordination between healthcare providers.

- **Remote Surgery Assistance Augmented Reality (AR):** AI-powered fog-edge computing is transforming telemedicine and remote surgery by delivering the ultra-low latency and precision these critical procedures demand. Edge devices at the surgical site process real-time sensor data, instrument movements, and AR overlays almost instantaneously, while fog nodes manage the heavy lifting of video compression, haptic feedback synchronization, and AI-driven image enhancement. This setup enables a surgeon located hundreds or even thousands of miles away to control robotic instruments with sub-millisecond precision, supported by AI tools that flag critical anatomical details or suggest procedural adjustments in real time. For example, in a rural clinic lacking specialist surgeons, an on-site medical team can collaborate with a world-class surgeon in a major city using AI-assisted AR glasses and robotic tools, ensuring life-saving care reaches remote or underserved communities. This combination not only bridges healthcare gaps but also expands access to expertise that would otherwise be out of reach.

Fog-Eege AI for Contactless Patient Care

AI-driven fog-edge computing opens new frontiers in contactless patient monitoring by combining innovative wireless technologies with edge intelligence. Using everyday tools such as WiFi network interface cards (NICs) equipped with specialized antennas and software, patient monitoring can extend beyond wearable devices to track vital signs such as breathing and heart rates, completely contact-free, as shown in Figure 3. This approach relies on the analysis of Channel State Information (CSI), which captures how WiFi signals are affected by the presence and movement of patients in a room. Tiny signal transmission disturbances caused by body movements or breathing patterns are detected and analyzed at the edge layer in real-time. AI models process these data locally, using advanced filtering techniques such as Hampel and median filters to remove noise, followed by feature extraction on parameters such as variance, skewness, kurtosis, and signal power. The fog layer aggregates and analyzes these signals, classifying human activities, such as standing, sitting, walking, falling, or lying down—with impressive accuracy. Tests using Single-Input-Single-Output (SIMO) and Multiple-Input-Multiple-Output (MIMO) antenna setups showed that MIMO configurations, especially when leveraging phase difference information, deliver superior performance in motion recognition.

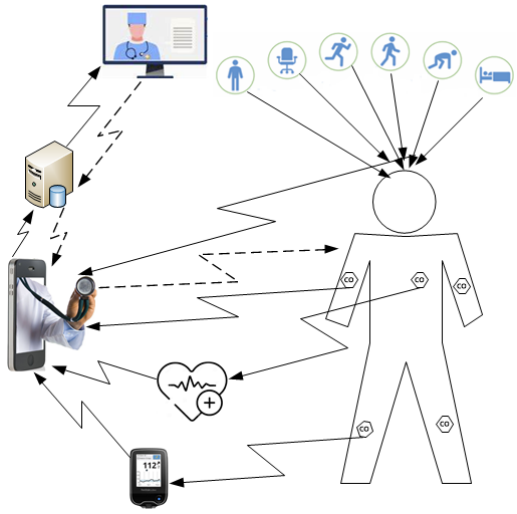

Figure 3: Fog-Edge AI for contactless patient care.

By embedding this AI-driven contactless monitoring system within a fog-edge architecture, hospitals and care facilities can achieve high precision in real-time, non-invasive patient observation while reducing the computational burden on cloud systems. This enhances patient comfort and safety and extends continuous monitoring to home settings, making it especially valuable for elderly care, post-surgery recovery, and chronic disease management.

Problem Formulations and Data Acquisition

While AI-driven fog-edge computing brings enormous potential to IoMT, several critical challenges and open issues must be addressed for it to achieve reliable, scalable, and ethical healthcare transformation:

- **Data Security:** AI at the edge and fog layers can improve real-time threat detection, encryption, and anomaly recognition to protect sensitive patient data. However, balancing strong security with the limited resources of IoMT devices remains a key challenge. Future work must focus on lightweight AI-powered security protocols, secure federated learning, and adaptive encryption to safeguard decentralized networks.
- **Interoperability:** AI models thrive on diverse data streams, but the fragmentation of IoMT ecosystems limits seamless data exchange. AI-driven standardization tools, middleware, and adaptive translators at the fog layer can help bridge gaps between heterogeneous devices, improving workflow efficiency and multi-vendor integration.
- **Reliability and Accuracy:** AI algorithms deployed at the edge must deliver accurate insights from noisy, real-world healthcare data. Ensuring clinical-grade performance demands rigorous testing, continuous validation, and AI self-monitoring mechanisms across distributed fog-edge nodes to avoid diagnostic errors or treatment delays.

- **Ethical Considerations:** AI-driven decisions in IoMT—such as patient risk predictions or treatment recommendations—raise ethical concerns around bias, transparency, consent, and data ownership. Embedding explainable AI (XAI) frameworks and patient-centric design into fog-edge systems is essential to ensure trust, fairness, and autonomy.
- **Regulatory Compliance:** AI-enhanced fog-edge architectures must meet global regulatory standards (HIPAA, GDPR) governing healthcare data privacy and security. This requires developing compliance-aware AI models, automated auditing tools, and governance frameworks at the fog layer to manage legal and ethical risks across regions efficiently.

By addressing these challenges, AI-driven fog-edge computing can unlock the full potential of IoMT, enabling secure, reliable, and intelligent healthcare solutions that improve patient outcomes and system resilience. Collaborative efforts between researchers, clinicians, tech developers, and regulators are vital to overcoming these barriers and driving innovation.

Conclusion

This paper presents a robust AI-driven fog-edge architecture that significantly advances the performance, security, and scalability of IoMT systems. The framework reduces latency and bandwidth consumption by processing critical patient data closer to the source, ensuring timely clinical decisions and improved patient outcomes. Integrating advanced AI algorithms enables precise data analysis and real-time anomaly detection, enhancing the system's responsiveness. Comprehensive security measures, including encryption, multifactor authentication, and blockchain, safeguard sensitive patient data from evolving cyber threats. Case studies demonstrate the framework's superior efmm,ficiency, reducing energy consumption and doubling the speed of threat detection compared to cloud-based models. The architecture's flexibility supports diverse applications, from emergency response and predictive maintenance to personalized treatment and contactless monitoring. Notably, the proposed system addresses key challenges such as interoperability, reliability, ethical concerns, and regulatory compliance. This research highlights the transformative potential of AI-fog-edge systems to reshape modern healthcare delivery. Future work will expand the framework's adaptability, ensure ethical AI integration, and foster broader adoption in global healthcare ecosystems.

Acknowledgments

This work was supported by the Provost's Research Fellowship Award grant code 23060, Zayed University, UAE.

References

A., A. H.; and Aldossary, M. 2021. Energy-efficient edge-fog-cloud architecture for iot-based smart agriculture environment. *IEEE Access*, 9: 110480–110492.

Abdulkareem, K. H.; Mohammed, M. A.; Gunasekaran, S. S.; Al-Mhiqani, M. N.; Mutlag, A.; and Mostafa, S. 2019. A review of fog computing and machine learning: concepts, applications, challenges, and open issues. *IEEE Access*, 7: 153123–153140.

Aguru, A. D.; Babu, E. S.; Nayak, S. R.; and Sethy, A., A.and Verma. 2022. Integrated industrial reference architecture for smart healthcare in the internet of things: A systematic investigation. *Algorithms*, 15(9): 309.

Akilan; Hariharan, U.; Prakash, I. B.; and Rajkumar, K. 2023. Exploring the impact and potential of the Internet of Medical Things (IoMT): A Comprehensive Review . In *Proceedings of the fifth International Conference on Advances in Computing, Communication Control and Networking*, 967–972. India: IEEE.

Alam, A.; Qazi, S.; Iqbal, N.; and Raza, K. 2021. *Fog, edge and pervasive computing in intelligent internet of things driven applications in healthcare: Challenges, limitations and future use*. Wiley-IEEE Press.

Arcas, G. I.; Cioara, T.; Anghel, I.; Lazea, D.; and Hangan, A. 2024. Edge offloading in smart grid. *Smart Cities*, 7(1): 680–711.

Awaisi, K. S.; Hussain, S.; Ahmed, M.; Khan, A. A.; and Ahmed, G. 2020. Leveraging iot and fog computing in healthcare systems. *IEEE Internet of Things Magazine*, 3(2): 52–56.

Bisio, I.; Fallani, C.; Garibotto, C.; Haleem, H.; Lavagetto, F.; Hamedani, M.; Schenone, A.; Sciarrone, A.; and Zerbino, M. 2025. AI-Enabled Internet of Medical Things: Architectural Framework and Case Studies. *IEEE Internet of Things Magazine*, 8(2): 121–18.

Demirel, B. U.; Bayoumy, I. A.; and Faruque, M. A. 2022. Energy-efficient real-time heart monitoring on edge–fog–cloud internet of medical things. *IEEE Internet of Things Journal*, 9(14): 71112472–12481.

Goel, A.; and Neduncheliyan, S. 2024. Health Monitoring and Diag nostic Platform Based on AI and IoMT Sensors: An Overview of Methodologies and Challenges. In *Proceedings of the 1st International Conference on Trends in Engineering Systems and Technologies (ICTEST-24)*. IEEE.

Hrnandez-Jaimes, M. L.; Martinez-Cruz, A.; Ramírez-Gutiérrez, K. A.; and Feregrino-Uribe, C. 2023. Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and cloud–fog–edge architectures. *nternet of Things*, 23: 100887.

Jain, R.; Gupta, M.; Nayyar, A.; and Sharma, N. 2021. *Fog Computing for Healthcare Environments, Signals and Communication Technology*. Springer.

K., S. N.; and Das, A. K. 2022. Energy-efficient fuzzy data offloading for IoMT. *Computer Networks*, 213: 109127.

Kim, B.; Lim, B. H.; Suh, B.; Ha, S.; He, T.; and Shah, B. 2023. Enabling Grant-Free URLLC for AoI Minimization in RAN-Coordinated 5G Health Monitoring System. *IEEE Internet of Things*, 10(19): 17356–17368.

Mukherjee, A.; Ghosh, S.; Behere, A.; Ghosh, S. S.; and Buyya, R. 2021. Internet of health things (IoHT) for personalized health care using integrated edge-fog-cloud network.

Journal of Ambient Intelligence and Humanized Computing, 12(1): 943–959.

Otoum, S.; Ridhawi, I. A.; and Mouftah, H. T. 2021. Preventing and Controlling Epidemics Through Blockchain-Assisted AI-Enabled Networks. *IEEE Network*, 35(3): 34–41.

S., G.; and Mukherjee, A. 2022. Strove: Spatial data infrastructure enabled cloud–fog–edge computing framework for combating covid-19 pandemic. *Innovations in Systems and Software Engineering*, 20: 727–743.

Shah, B.; Junaid, M.; and Habib, M. 2024. Enhancing IoT Protocol Security through AI and ML: A Comprehensive Analysis. In *Proceedings of the International Symposium on Networks, Computers and Communications*, 1–7. Washington DC, USA: IEEE.

Tai, Y.; Zhang, L.; Li, Q.; Zhu, C.; Chang, V.; and Rodrigues, J. C. 2022. Digital-Twin-Enabled IoMT System for Surgical Simulation Using RAC-GAN. *IEEE Internet of Things Journal*, 9(21): 20918–20931.

Zhang, J.; Ouda, A.; and Abu-Rukba, R. 2024. Authentication and key agreement protocol in hybrid edge–fog–cloud computing enhanced by 5G networks. *Future Internet*, 16(6): 209.

Zhang, P.; Chen, W.; Shen, S.; Yu, S.; Kumar, N.; and Hsu, C. 2024. I-Enabled Space-Air-Ground Integrated Networks: Management and Optimization. *IEEE Network*, 38(2): 186–192.