International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol. 9, No. 3, 2022, pp. 11-15.

ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

Fog and Edge Computations for Real-Time Healthcare Data Processing in IoT Applications

Seema Reddy [a], Parth Jaiswal [b]

[a] *Augmented Intelligence Unit, Nagpur Centre for AI Research, India.*
[b] *Augmented Intelligence Unit, Nagpur Centre for AI Research, India.*

Abstract

The Internet of Things (IoT) is producing a substantial amount of information. Fog and edge computing (FEC) enables remote storage and analysis of medical sensing and actuator information through distributed computers. The results thereafter be transmitted through the Internet. The quantity of devices in the IoT encompasses many wireless diabetic devices, including blood glucose tracks, continual glucose monitoring, insulin pencils, pumps for insulin, and systems with closed loops. The FEC paradigm for storing and analyzing data is becoming incapable of managing the data deluge, necessitating the delegation of processing to the network's edge, nearer to the data-generating devices. FEC at the edge are two frameworks for data management that facilitate the offloading of data from the cloud, enabling localized processing near the patient and facilitating communication within moments or minutes. Information from sensors can be processed proximate to the detecting and actuation devices utilizing fog computing (via local routers) and edge computing (inside the sensing equipment). Nearly all connected diabetic devices utilize FEC due to the necessity for immediate responses to sensor input, as individuals cannot endure delays associated with cloud computing.

Keywords: Fog, Edge, Healthcare, Internet of Things.

DOI: 10.71086/IAJSE/V9I3/IAJSE0922
Received: 10 June 2022/Revised: 11 July 2022/Accepted: 20 August 2022/Published: 30 September 2022

Introduction

The Internet of Things (IoT) (Laghari et al., 2021) and Fog and Edge Computing (FEC) (Omoniwa, et al., 2018) concepts have instigated a technological revolution in the contemporary economy, facilitating an Internet-based framework for advancing numerous intelligent medical services. Employing such innovations in the Smart Healthcare System (SHS) (Algarni, 2019) can enhance the quality of care, treatment processes, and healthcare service costs. IoT devices produce a substantial volume of patient information stored on a computer and disseminated among healthcare experts for treatment reasons. The handling of this data poses a considerable challenge for the advancement of real-time response systems. Concurrently, the e-healthcare system requires architectural solutions that uphold service continuity, security, minimal latency, network capacity, and the inherent characteristics of the network. These solutions encompass FEC, portable cloud computing (Huo et al., 2018), fog-based computing (Wang et al., 2018), microdata centers, cloudlets, cloud-sea calculating, and edge computing for mobile devices.

In the research, most e-healthcare systems are predicated on the cloud, wherein the gateway is positioned in a standalone and autonomous manner. All healthcare data and services are hosted on a cloud server and accessible via the World Wide Web. Wireless Body Sensor Networks (WBAN) (Zuhra et al., 2017) are utilized in the medical field by applying cloud computing principles. It facilitates real-time health monitoring remotely via implantable intelligent gadgets or detectors on the human body. Numerous FEC systems have been deployed to enable the remote monitoring of patients. Expeditious treatment solutions and replies are essential for the efficacy of such a system. For example, in the surveillance of critical patients, elevated network latency and response times result in treatment delays, potentially culminating inpatient mortality.

FEC systems are ineffective in health care due to significant service latency and inefficient use of computer resources resulting from the extensive distance between the user and the cloud center. FEC capacities are insufficient for processing vast amounts of data from diverse sources across many networks. The network capacity and transmission speeds diminish due to multiple user access demands. Remotely stored information is susceptible to security and privacy concerns. Control of access and data leakage are prevalent issues in online computing. The data is often encrypted before uploading to the internet to safeguard it from potential attackers. This ensures the data's security. However, conducting a search operation on such encrypted information can be challenging. Each instance necessitating complete encryption or decoding can lead to substantial bandwidth consumption, increased overhead, and inadequate storage capacity. Conventional cloud-based computing options are insufficient for meeting the service demands of applications in real-time, such as remote healthcare in emergencies.

Related Studies

An extensive examination of medical privacy and data security inside the edge computing framework is presented. They have examined security concerns and assaults within the edge computing ecosystem. Promising protective and countermeasure methods, such as cryptography-based solutions, have emerged to secure systems reliant on edge computing. However, the processing time for cryptography-based systems is considerable.

The potential of FEC techniques in healthcare IoT systems is examined. The classification results of the research provide many methods and approaches to facilitate fog computing-based applications for healthcare. The Deep Learning (DL) (Zhang, et al., 2020) approach is employed in an interconnected IoT and FEC context to develop a Smart Healthcare System (SHS). The HealthFog system offers lower-latency and energy-effective processing options. This system autonomously diagnoses cardiac illnesses and effectively handles the data of cardiac patients.

A research team has built a real-time e-healthcare tracking system based on Fog and IoT technologies. The suggested monitoring system leverages the benefits of cloud-to-fog (C2F) Computer science, including edge data storage, expedited analysis of data, real-time information dissemination, and reduced reaction times.

A fog-cloud computer framework including a sensor, fog, and internet layer is utilized to develop large-scale IoT-based medical applications. This program administers tailored healthcare services, enhancing operational efficiency and minimizing reaction time. Optimization designs, including partitioning, clustering, interaction, and parallel processing, are utilized to improve system effectiveness.

A safe SDN-based edge computing structure for IoT-enabled medical facilities has been established. All IoT devices at the edge server have been verified using a lightweight security method. All data is transmitted for storage, processing, and analysis. The Software-Defined Networking (SDN) (Benzekki, et al., 2016) controller interfaces with the edge server and is tasked with distributing load, optimizing networks, and using practical resources in IoT-enabled medical facilities. Device security is a critical concern in FEC ecosystems. The study presented a cybersecurity architecture for identifying rogue edge gadgets to address this issue. They have employed three security designs: the Markov model, the Intrusion Detection System (IDS), and the Virtual Honeypot Device (VHD) to enhance system safety and the precision of malicious node identification.

The potential of fog computing techniques in healthcare IoT systems is examined. The taxonomy discovered in the literature provides many methods and approaches to facilitate fog computing-based medical applications. The DL approach is utilized in an integrated IoT and fog computing context to develop SHS. The Health Fog system offers lower-latency and energy-effective processing options. This system autonomously diagnoses cardiac illnesses and effectively handles the data of cardiac patients.

A study has built a real-time e-healthcare tracking system based on Fog and IoT technologies. The suggested surveillance system leverages C2F Computing attributes, including edge data storage, expedited processing of data, immediate data dissemination, and reduced response times. A fog-cloud computer framework including a sensor, fog, and cloud level is employed to develop large-scale IoT-based medical applications. This program administers individualized healthcare services, enhancing efficiency and decreasing response times. Optimization designs, including partitioning, clustering, interaction, and parallel computation, are utilized to improve system effectiveness. An IoT system enhanced by FEC has been created to track remote diabetes patients. Energy-efficient nodes for sensors in FEC at the network border can monitor crucial human indicators, including glucose levels, body heat, and environmental contextual information such as ambient temperatures, moisture, and air conditions. The safe cryptographic technique safeguards the acquired data.

A safe SDN-based computing system for IoT-enabled medical facilities has been established. All connected devices at the edge of the computer are authenticated with a lightweight security method. All data is transmitted for storage, processing, and analysis. The SDN controller interfaces with the FEC, distributes load, optimizes networks, and uses practical resources in IoT-enabled medical facilities.

The safety of devices constitutes a critical concern in the fog computing and cloud-of-things ecosystems. The study presented a cybersecurity architecture for identifying rogue edge equipment to address this issue. They have employed three safety examples: the Markov approach, the IDS, and the VHD to enhance system safety and the precision of malicious node identification.

Fog and Edge Computations for Real-Time Healthcare Data Processing

The given research challenge formulates the suggested framework. It comprises two modules: the Encryption module and the Access Control component. An SHS incorporates an edge computer layer between the mobile body sensors and the data servers in the suggested design. This computing level minimizes response time and facilitates prompt decision-making for real-time analysis. This component implements encryption, ensuring secrecy and safeguarding patient data confidentiality. This strategy involves partitioning and encrypting data into different segments, allowing access solely to a subset of texts that include the user's specified keyword. People search for secret information without decryption throughout the access period. During this procedure, only pertinent data are visible due to only one keyword-based searchable password method, while the remaining data are encrypted.

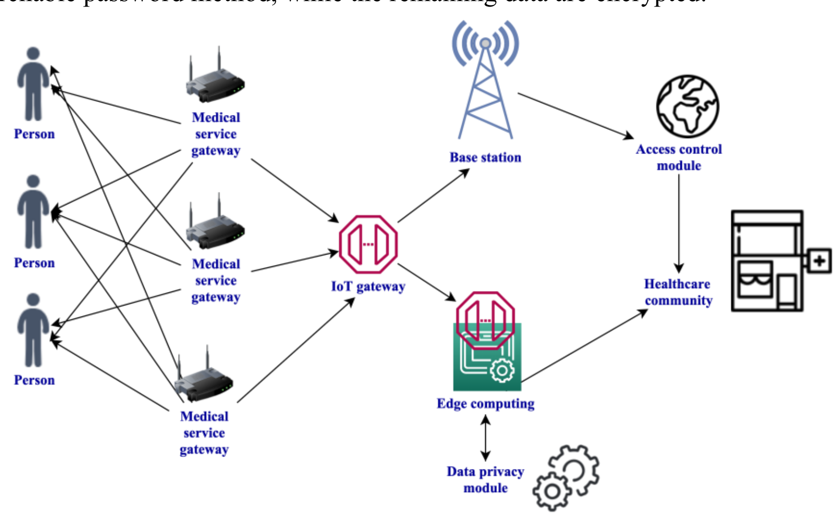


Fig. 1: Edge computing model in competent healthcare

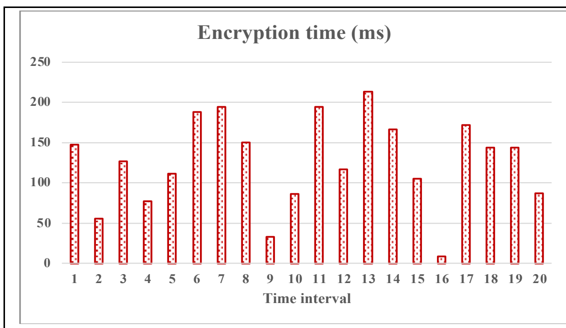
The access management model is executed on the information storage computer, enabling the restriction of unwanted access. The proposed pair of modules will function in this manner. The FEC structure operates at three distinct levels. 1) Sensor levels - gathering information from the edge gadget; 2) Networking coordinator stage - numerous linked devices transmit data to the edge processor nodes; 3) Decision-making levels - the layer of edge computing processes data within minutes for decision-making. Fig. 1 illustrates the overall design of the suggested secure paradigm.

This framework facilitates interactions across many entities for specialized functions such as data capture, aggregation, storage, and analysis, all while ensuring data privacy is maintained. Below is a description of each entity:

- Intelligent Users are individuals in good health. Geriatric clients, severely ill individuals, inpatients, physicians, nurses, laboratory workers, etc. Biosensors are inserted in patients' bodies to gather biological signals, which are aggregated in IoT gadgets and kept in encrypted form in cloud storage.
- Edge Bridge immediately processes minor data collected from the intelligent patient society. This localized data diagnostic is intended to regulate smart devices such as cardiac pumps and oxygen delivery systems. It encrypts the information and stores it in cloud storage for subsequent analysis, which physicians can access during treatment.
- Database Administrator is primarily accountable for data storage and handling of queries. The executed query will retrieve the key for encryption from the key creator.
- Edge Servers will oversee all data assets from various competent society members and categorize them into distinct clusters for analysis in their secured state.

Results

The encryption duration is quantified in another time interval, as depicted in Fig. 2. The calculated findings indicate that the duration fluctuates with each period. It primarily depends on the volume of patient information. The experiment's findings suggest that the mean encryption duration is 130 microseconds, minimal for encrypting patient information. The efficiency of every FEC node tasked with processing patient data is tracked. The processing speed of the FEC node determines the rate of successful computations within the layer of edge computing over a specified period. Fig. 3 illustrates the throughput of every edge of the nodes. Experimental findings indicate that the model's median speed is 210 kbps.



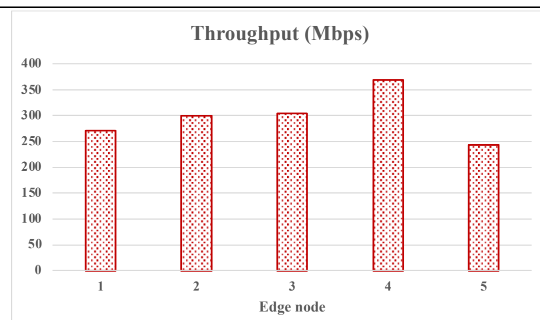
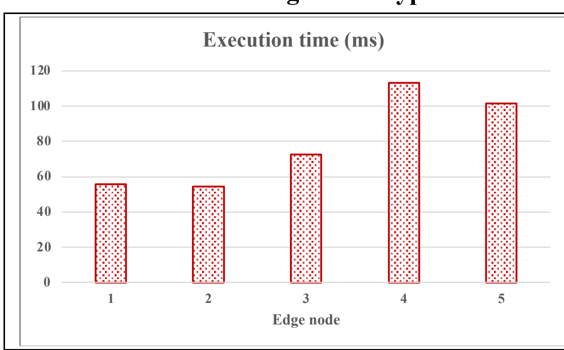


Fig. 2. Encryption time analysis and Fig. 3. Throughput analysis



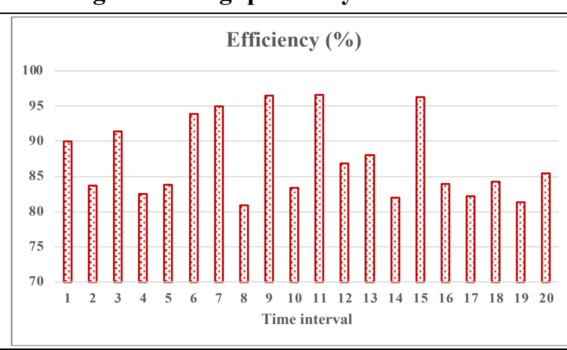


Fig. 4. Execution time analysis and Fig. 5. Efficiency analysis

The volume of data received and transferred post-encryption directly influences the processing time of the FEC networks. The time required for the execution of the edge nodes fluctuates due to variations in their execution speeds. The execution time depends on the workload and congestion at the edge nodes. Fig. 4 illustrates the execution duration of all five node edges. The visualizations indicate that the mean time for processing the FEC computer layer is 110 milliseconds. The practical application of the suggested framework is utilized to assess the simulation outcomes regarding hardware and FEC node effectiveness. The proposed approach was evaluated across different periods, yielding varying levels of effectiveness. The findings differ owing to the system's diverse characteristics and diversity among the edge computing units. The findings demonstrated that the system attained an efficiency of up to 94%. This effectiveness encompasses both hardware and node performance. The findings of the efficacy gained are presented in Fig. 5.

Conclusion

FEC will gain significance as the subsequent advancement beyond cloud computing. This model will be integral to the forthcoming 5G Mobile Communication Network, now in construction. The 5G mobile networking will have enhanced speed, reduced latency, and less energy consumption than the existing fourth-generation (4G) network. FEC is anticipated to be a crucial facilitator of processes requiring swift responses to sensor inputs, including wireless health surveillance, augmented and autonomous vehicles, robotics, drones, and locating missing children. As the volume of information produced by the IoT escalates, particularly diabetes-related information, the demand for FEC utilizing fog and edge computing designs will steadily rise.

References

Laghari, A. A., Wu, K., Laghari, R. A., Ali, M., & Khan, A. A. (2021). A review and state of art of Internet of Things (IoT). *Archives of Computational Methods in Engineering*, 1-19. https://doi.org/10.1007/s11831-021-09622-6.

Omoniwa, B., Hussain, R., Javed, M. A., Bouk, S. H., & Malik, S. A. (2018). Fog/edge computing-based IoT (FECIoT): Architecture, applications, and research issues. *IEEE Internet of Things Journal, 6*(3), 4118-4149. DOI: 10.1109/JIOT.2018.2875544.

Algarni, A. (2019). A survey and classification of security and privacy research in smart healthcare systems. *IEEE Access, 7,* 101879-101894. DOI: 10.1109/ACCESS.2019.2930962.

Huo, Y., Blaber, J., Damon, S. M., Boyd, B. D., Bao, S., Parvathaneni, P., ... & Landman, B. A. (2018). Towards portable large-scale image processing with high-performance computing. *Journal of digital imaging, 31,* 304-314. https://doi.org/10.1007/s10278-018-0080-0.

Wang, T., Zhou, J., Liu, A., Bhuiyan, M. Z. A., Wang, G., & Jia, W. (2018). Fog-based computing and storage offloading for data synchronization in IoT. *IEEE Internet of Things Journal*, *6*(3), 4272-4282. DOI: 10.1109/JIOT.2018.2875915.

Zuhra, F. T., Bakar, K. A., Ahmed, A., & Tunio, M. A. (2017). Routing protocols in wireless body sensor networks: A comprehensive survey. *Journal of Network and Computer Applications*, *99*, 73-97. https://doi.org/10.1016/j.jnca.2017.10.002.

Zhang, Y., Doshi, A., Liston, R., Tan, W. T., Zhu, X., Andrews, J. G., & Heath, R. W. (2020). Deep WiPHY: Deep learning-based receiver design and dataset for IEEE 802.11 ax systems. *IEEE Transactions on Wireless Communications*, *20*(3), 1596-1611. DOI: 10.1109/TWC.2020.3034610.

Benzekki, K., El Fergougui, A., & Elbelrhiti Elalaoui, A. (2016). Software-defined networking (SDN): a survey. *Security and communication networks*, *9*(18), 5803-5833. https://doi.org/10.1002/sec.1737.