WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Impact of Edge-Based Mobile Cloud Computing Solutions in Smart Health Care System

Suneetra Chatterjee[1], Dr. Harsh Lohiya[2]

[1]Research Scholar, Sri Satya Sai University of Technology and Medical Sciences, Sehore (M.P.), India
[2]Associate Professor, Sri Satya Sai University of Technology and Medical Sciences, Sehore (M.P.), India

ABSTRACT

EMCC harnesses the computational prowess and storage capabilities of edge devices and cloud resources to tackle security issues in IoT environments. Task distribution to the network edge minimizes data transmission to the cloud, mitigating latency issues and augmenting privacy measures. EMCC adopts a decentralized strategy to minimize the exposure of sensitive information to potential threats. The edge infrastructure integrates state-of-the-art security mechanisms, including secure data aggregation, cryptographic algorithms, and access control mechanisms. Robust key management and authentication protocols are implemented to ensure secure communication among IoT devices, edge nodes, and cloud servers. By offloading computational tasks to the edge, EMCC eases the load on resource constrained IoT devices, leading to optimized energy consumption and prolonged device lifespan. Cloud resources offer scalability, enabling seamless expansion of IoT deployments while maintaining a strong security posture. EMCC not only tackles security challenges but also enhances the performance of IoT systems, making it a compelling choice for forthcoming IoT deployments.

Keywords: Edge Computing, IoT Security, Mobile Cloud Integration, Network Paradigms, Security Enhancement.

1. Introduction

In the domain of computing power and response time, modern and next-generation healthcare services present a unique set of demands. These sophisticated devices require swift and energy-efficient computing, expanded storage capacity, and location awareness, challenges that conventional cloud computing struggles to meet. Fog computing, alternatively termed "edge computing" following N. Bonomi's proposition, emerges as a promising technology, signifying the decentralization of computing to the network's edge.

The precursor to edge computing, mobile cloud computing (MCC), is marked by high data transmission costs, prolonged response times, and limited coverage. Cloudlet and local cloud, akin computing methods, offer subpar Quality of Service (QoS) for contemporary devices. Elevated costs associated with data transmission result from increased network traffic, impacting transmission times. While cloudlet-based solutions exhibit lower latency than MCC, they still fall short in providing necessary mobility for devices due to limited Wi-Fi coverage. Comparative studies consistently show that only edge-based computing can meet contemporary requirements for latency, mobility, and energy efficiency.

The healthcare sector stands to gain significantly from the enhanced performance of edge computing. Edge-based solutions offer reduced latency for time-sensitive applications such as vital sign monitoring and fall detection for the elderly. Furthermore, they bolster security, allowing for the secure transmission of sensitive health data to caregivers, including information such as blood pressure, heart rate, blood sugar, and health history. The advancements in tracking and mobility facilitated by edge computing enable healthcare providers to offer personalized care for individuals with chronic illnesses in their homes, leveraging ambient sensors and wearable vital sign sensors for comprehensive data collection both indoors and outdoors.

To deliver real-time, quality service to patients, edge devices and nodes must execute data operations with low latency, energy efficiency, location awareness, and an elevated level of security. This survey's primary objective is to identify specific data operation techniques ensuring optimal performance in an edge-based healthcare system. This information can guide the selection of optimal classification, authentication, encryption, and data reduction methods for deploying edge devices. The subsequent sections of this paper will cover various topics, including a review of current surveys on healthcare, an exploration of healthcare applications and their quality of experience requirements, an examination of cloud and cloudlet-based solutions, insights into edge-based solutions and their architecture, and a taxonomy of edge computing-enabled healthcare categorized by data operation meeting 5G performance targets. The paper will conclude with discussions on open research areas and challenges.

The mobile healthcare systems have been applied widely because of the advances in biotechnologies, information technologies and software engineering. Due to pervasive e-health services, billions of personal healthcare data records are generated annually. Users interact with healthcare service providers frequently in current applications, e.g., mobile telemedicine, personalized medicine, and emergency response. Towards secure interaction, a tremendous amount of healthcare data should be collected and processed well. Besides, healthcare data is a valuable commodity for public health agencies, academic

researchers, and pharmaceutical companies to promote service provision, including disease prevention and control, healthcare-related research, and drug development, via big data analytics. Common business cases for data mining in mHealth include Google. To develop diagnostic applications, Deep Mind's subsidiary collects and analyzes medical data from 1.6 million patients in hospitals in London. To begin effective data analysis, third parties must gain authorized access to medical data. As data owners, we need data transactions to negotiate with users. As a result, there are significant challenges in managing multiple health data safely and efficiently. To tackle the problems, some of existing work pay attention to centralized data management with cloud computing in mobile healthcare systems. Centralized data management leads to high-latency response and excessive workloads when the central authority continuously processes a lot of healthcare data over time. The central authority also easily suffers from typical single point failure, DDoS attacks and remote hijacking attacks. So, most of the work have begun to focus on decentralized data management for performance improvement in recent years. They leveraged the blockchain technology which is a peer-to-peer distributed ledger to prevent any repudiation in the trust less environment and achieve self-organized and transparent management by depending on a set of consensus nodes. Their goal was to make it easier to manage dependable, verifiable, and traceable data in the healthcare industry.

Objective:

Edge-based mobile cloud options are meant to make IoT devices safer, which is one of their goals.

1. Create a system for mobile cloud computing that is based on the edge. The main goal is to create and build a mobile cloud computing platform that is dependable, scalable, and easy to use and can talk to IoT devices. This framework needs to be able to move computing jobs from IoT devices to edge servers in a safe way. This will make the Internet of Things more secure.
2. Installing extra security steps on edge servers can protect the information that moves between IoT devices and the cloud. This can be done by making the barriers around the area even stronger. Security measures like data encryption, user ID/password authentication, limited access, and breach detection are used to keep data safe while it is in transit.
3. Secure communication methods need to be thought up and put into place to make sure that data sent between edge servers and IoT devices stays private and is not changed. To stop unauthorized access and data breaches, these systems should use encryption and strong authentication methods. The main goal of this project is to set up a safe and reliable way to communicate that makes it less likely that data will be stolen or changed in some other way.
4. By designing and putting in place the right methods on edge servers, it is possible to store and manage data in a secure way. Anonymizing data, sharing data in a safe way, and processing data in a safe way are all ways to protect classified information while making it easier to use and analyze data. The goal is to find a good balance between making sure data is safe and making sure it can be processed quickly enough to let IoT devices make decisions in real time.
5. Build IDPS (Intrusion Detection and Prevention Systems): Install innovative intrusion detection and prevention systems on the edge servers to find and stop any security risks. To find and stop malicious behaviour in real time, you need tools for network tracking, algorithms for finding outliers, and ways to use machine learning. For the security of the data and for the Internet of Things system to keep working right, it is important to take precautions against risks.
6. Do a lot of performance studies to figure out how effective and scalable edge-based mobile cloud computing systems are. By keeping an eye on things like response time, throughput, resource usage, and scalability, you can see if the suggested security changes could hurt the overall performance of the system. When working in an IoT setting, it is important to find a good mix between speed and security.
7. Case studies can be used to prove that the method works: Use IoT use cases from the real world to evaluate how well the mobile cloud computing solution at the edge works. Work with partners in the industry and put the answer to the test in several use cases to get feedback and figure out if it is viable, effective, and scalable. To reach this goal, it is important to make sure that the suggested security changes work and are useful in real-world Internet of Things situations.
8. Give some ideas and examples of how to do things right: IoT systems need to produce standards and best practices for setting up and taking care of mobile cloud computing solutions at the edge of the network. These guidelines should talk about security problems, how to set up the system, and how to take care of it to help businesses make and keep IoT systems safe. This document aims to set up a road map for the growth of edge-based mobile cloud computing solutions so that more people can use them.

Edge-based mobile cloud computing solutions are often the best way to protect the privacy, integrity, and availability of data while also making it easy to manage and analyses it in real-time Internet of Things (IoT) settings. These are the most important ones.

2. Literature Review

Dr. Suresha K, et al. (2023) This survey gives an overview of edge computing. It talks about its general architecture, its key parts, and some of the ways it can be used. It also looks at some of the problems that could come up when putting edge computing into place, as well as some of the possible ways that this technology could go in the future.

Hagan, M.et al.(2020) The goal of this study is to improve the privacy and security of edge computing systems for the next generation. The writers talk about the problems and dangers of edge computing and give ways to solve them. Edge computing environments have a lot of potential security and privacy problems. These pieces investigate these worries and offer workable solutions, such as secure communication protocols, access control systems, and data encryption strategies. With this study, we hope to lay the groundwork for making edge computing setups safe and private for end users.

Fazeldehkordi, E., et al. (2022). This study looks at security architectures for the Internet of Things (IoT) that are built on edge computing. The writers look at several different security strategies and architectures that can be used to protect IoT devices and data in edge computing environments. They offer several architectural ideas, such as device-level security, edge gateway security, and cloud-edge integration, to solve the problems and meet the needs of safe edge computing on the Internet of Things. The results of this poll give interesting information about how secure edge-based Internet of Things (IoT) devices are right now.

Jeon, G.et al. (2022). This study investigates the idea of "intelligent mobile edge computing" and what role it plays in managing the enormous amounts of data that Internet of Things devices create. It lays the groundwork for efficient data processing and analysis at the edge, which lets IoT apps act in real time.

Masarweh M, et al. (2022) This study looks at how well fog computing, cloud computing, and the Internet of Things environment could work together. By combining cloud computing and fog computing, it creates a sophisticated broker management solution that makes it easier for decentralized IoT systems to share resources and handle data.

Brecko A, et al. (2022) This survey looks at how federated learning can be used in edge computing situations. This piece talks about the pros and cons of federated learning in edge contexts and shows how different strategies and techniques are used for distributed model training and inference.

Qiu, T.et al. (2020). This survey report is mostly about the idea of "edge computing" in the framework of the IIoT. In this essay, the writers talk about the architecture, progress, and problems of edge computing in IIoT deployments. They talk about the basics of edge computing systems and look at some ways they could be used in business. The study also talks about the security measures and methods that can be used to keep data safe in edge computing. It shows how the Internet of Things (IoT) poses unique risks to data protection. The study gives an in-depth look at edge computing as it relates to the Internet of Things in industry.

Abdulmalik Alwarafy et al. (2020) did a thorough study of the privacy and security problems that produce IoT that uses edge computing. The authors talked about separate ways to keep edge computing and IoT devices safe and pointed out the biggest problems in this area. Some of the security risks they talked about were data privacy, network attacks, and device authentication. They also made some suggestions for more study.

Sha et al. (2020) IoT security methods based on edge computing were investigated as part of a study. They talked about the pros and cons of using edge computing to improve the security of IoT. Some of the methods and approaches that the writers have looked at in depth are secure data aggregation, edge-based intrusion detection, and secure communication protocols. They also talked about how edge computing systems need to have security measures that work together.

3. Proposed Work and Result Discussion

Securing Healthcare IoT Systems

Hosted mobile cloud healthcare information systems improve the security of the Internet of Things.

As the Internet of Things (IoT) continues to change the healthcare business, it is becoming more important to protect patient privacy while making sure it is available. Using edge-based mobile cloud computing solutions is a safe way to make IoT systems in healthcare more secure. The processing and storage powers of edge devices, such as smartphones and wearables, can be used by health care workers to manage sensitive data locally. Because of this, there is less chance of a security breach or other unwanted entry. The benefits of edge-based mobile cloud computing in healthcare systems are looked at, and a wide range of security choices for protecting IoT infrastructures from attacks are talked about.

When Internet of Things devices are added to current healthcare systems, it makes it possible to monitor patients in real time, manage them from a distance, and give them personalized care. The enormous amounts of potentially personal data that these gadgets create, on the other hand, pose major risks to the privacy of information. Edge-based mobile cloud computing solutions offer a decentralized and safe architectural framework to deal with these problems. The paper's problem statement and goals are quickly explained below.

a. Cloud computing on the edge and on mobile devices for the healthcare industry

In the next few lines, we will talk about the idea of "edge computing" and how it might be used in healthcare systems. This shows how important it is to use devices on the edge, like smartphones and wearables, as computing and storage tools for processing and analyzing medical data. By combining mobile cloud computing with edge devices, healthcare systems can grow and work better.

b. Concerns about the safety of medical devices that can connect to the internet.

Here, we will look at some of the concerns people have made about the safety of healthcare IT that uses the internet. This piece talks about the risks that come with data breaches, how IoT devices can be vulnerable, and what could happen if healthcare data is exposed. Privacy problems and the difficulties of meeting rules are also talked about.

c. Cloud computing on mobile devices at the edge to improve internet security.

In this part, we talk about different security options that can be used with edge-based mobile cloud computing to ease worries about the safety of IoT healthcare systems. Authentication methods, access control systems, authentication algorithms, and data encryption are some of the things that are talked about here. Integration of trusted execution environments and private enclaves on edge devices is also studied.

d. Examples of research and how professionals do it

This part gives examples of how edge-based mobile cloud computing has been used in the real world and makes suggestions for best practices. It gives examples of installations that have helped improve health, business output, and safety. Case studies show a wide range of uses, such as watching patients from afar, giving each person their own care, and analyzing data.

e. What the future holds and how to get through hard times

Here, we will look at where cloud computing in healthcare is going and what new things might happen in edge-based mobile cloud computing. It looks at how innovations like 5G networks, AI, and blockchain could affect how IoT healthcare systems can grow and how safe they are. Both the possibilities for future study and the current problems in this field are brought to light.

Healthcare IoT System Diagram	
IoT Device 1 - Authentication - Data Encryption - Secure Boot- Firmware Integrity	IoT Device 2 -Authentication -Data Encryption - Secure Boot -Firmware Integrity
Network- Segmentation- Firewalls Intrusion Detection	
Compliance Checks HIPAA Compliance- Regulations	
Data Storage- Encryption (at rest)	
Security Analytics – Monitoring - Anomaly Detection	
User Authentication and Authorization - Role-based access control	
Compliance Checks - HIPAA Compliance - Regulations	
Vendor Assessment - Security Audits - Best Practice	
Incident Response	
- Plan and Protocols - Communication	

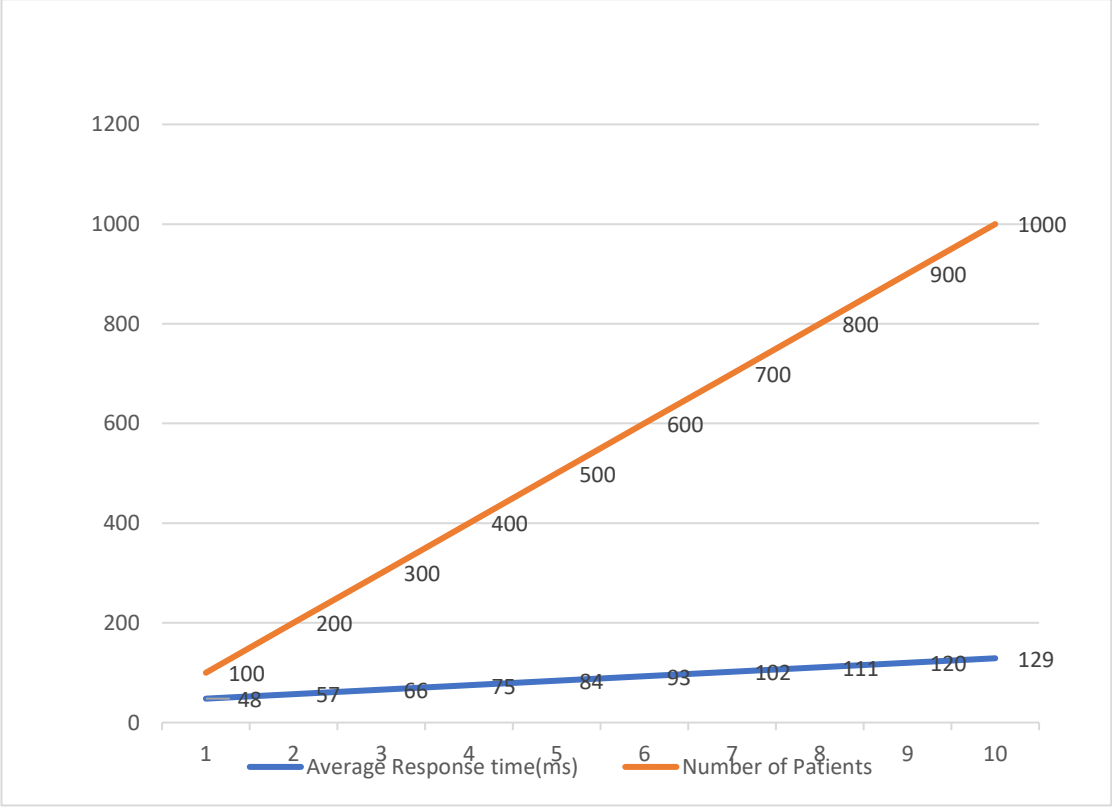

Figure 1: Impact of EBMCC in Healthcare system

The distributed structure in the context of the Internet of Things (IoT) offers several advantages, although it is not explicitly outlined in the provided text. However, the primary focus of the discussion revolves around the security and privacy challenges associated with this distributed architecture.

Regarding privacy concerns, the text suggests that edge computing could serve as an effective platform for future IoT systems. By processing data at the edge, closer to the data source, there is potential for better protection of privacy-sensitive information related to end users. Notably, the text highlights a potential vulnerability: the storage of sensing data at edge nodes, which may be more susceptible to security breaches compared to centralized cloud servers.

To address privacy issues in edge computing, the text recommends implementing effective privacy-preserving mechanisms. Two specific approaches mentioned are local differential privacy and differential privacy with high utility. These mechanisms are designed to ensure the protection of user privacy within the environment of edge computing based IoT.

Switching the focus to security challenges, the text identifies one common issue in edge computing—authenticating gateways at various levels. The example provided illustrates this concern with smart meters in residential homes, each possessing its unique IP address.

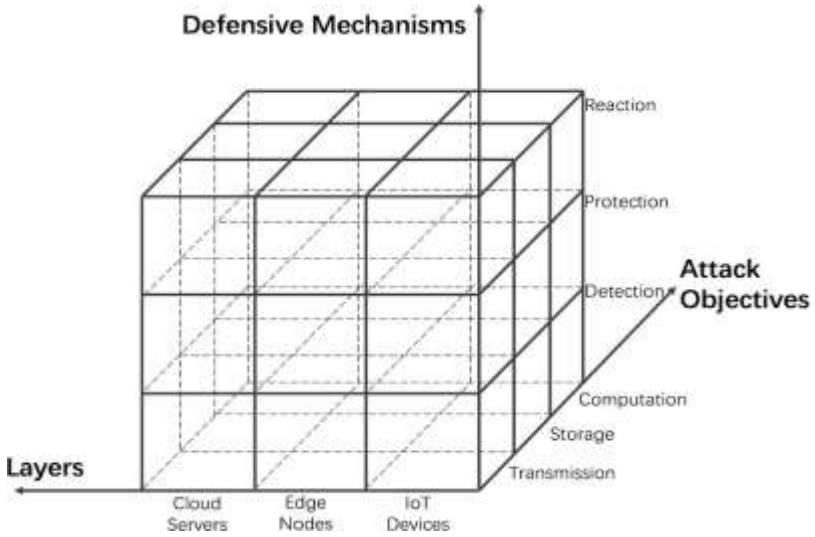

Figure 2: Working of layers using defensive mechanisms

In conclusion, the text underscores the critical importance of addressing security and privacy challenges within the distributed structure of IoT. While edge computing is presented as a potential solution to enhance privacy, it also introduces new security considerations, such as gateway authentication. The recommendation is to implement tailored privacy-preserving mechanisms to safeguard user privacy effectively in the evolving landscape of edge computing-based IoT environments.

4. Conclusion

Edge computing also makes it possible to control and keep an eye on edge-level security. At the edge of the network, security policies and updates can be set up and enforced. This makes it easier to keep an eye on connected devices and make sure they follow security rules. This method improves the security of the IoT ecosystem as a whole and makes it more resistant to threats.

But it is important to remember that edge-based mobile cloud computing options are not perfect. Distributed edge computing makes it harder to keep track of and coordinate security steps for all the devices that make up the edge network. It is important to make sure that the edge infrastructure is safe so that it does not get hacked and let people in who should not be there.

Using mobile cloud computing solutions at the edge of the network is an effective way to make the Internet of Things (IoT) safer. We can fix the security problems that IoT devices have by giving standards top priority and making usage plans. As the ecosystem of the Internet of Things (IoT) continues to grow, edge-based mobile cloud computing can make IoT systems much safer. This goal can be reached by using encryption to send data, putting in place intrusion detection and protection systems, and building a culture of trust and identity management.

In conclusion, the most important study findings are summed up, and edge-based mobile cloud computing solutions are stressed to improve the security of IoT healthcare systems. This article talks about how patient care could get better, costs could go down, and medical studies could get bigger.

REFERENCES

1. Hagan, M., Siddiqui, F., & Sezer, S. (2020). Enhancing Security and Privacy of Next-Generation Edge Computing Technologies. In 2019 17th International Conference on Privacy, Security and Trust, PST 2019 -Proceedings (International Conference on Privacy, Security and Trust

(PST)). Institute of Electrical and Electronics Engineers Inc.https://doi.org/10.1109/PST47121.2019.8949052 https://doi.org/10.1109/PST47121.2019.8949052.

2. Brecko A, Kajati E, Koziorek J and Zolotova I. (2022). Federated Learning for Edge Computing: A Survey. Applied Sciences. 10.3390/app12189124. 12:18. (9124). https://www.mdpi.com/2076-3417/12/18/9124.
3. Qiu, T.; Chi, J.; Zhou, X.; Ning, Z.; Atiquzzaman, M.; Wu, D.O. Edge computing in industrial internet of things: Architecture, advances, and challenges. IEEE Commun. Surv. Tutor. 2020, 22, 2462–2488.
4. Fazeldehkordi, E.; Grønli, T.-M. A Survey of Security Architectures for Edge Computing-Based IoT. IoT 2022, 3, 332-365. https://doi.org/10.3390/iot3030019.
5. Al Masarweh M, Alwada'n T and Afandi W. (2022). Fog Computing, Cloud Computing, and IoT Environment: Advanced Broker Management System. Journal of Sensor and Actuator Networks. 10.3390/jsan11040084. 11:4. (84). https://www.mdpi.com/2224-2708/11/4/84.
6. Dr Suresha K, Suresh Goure, Shaheen Banu. A Comprehensive Review of Edge Computing. DOI Link: https://doi.org/10.22214/ijraset.2023.48484.
7. Jeon, G., Albertini, M., Bellandi, V. et al. Intelligent mobile edge computing for IoT big data. Complex Intell. Syst. 8, 3595–3601 (2022). https://doi.org/10.1007/s40747-022-00821-7.
8. Kewei Sha, T. Andrew Yang, Wei Wei, Sadegh Davari. A survey of edge computing-based designs for IoT security. Digital Communications and Networks, Volume 6, Issue 2, May 2020, Pages 195-202. https://doi.org/10.1016/j.dcan.2019.08.006.
9. Abdulmalik Alwarafy, Khaled A. Al-Thelaya, Mohamed M. Abdallah, Schneider. A Survey on Security and Privacy Issues in Edge Computing-Assisted Internet of Things August 2020.