Volume: 12 **Issue:** II **Month of publication:** February 2024

DOI: https://doi.org/10.22214/ijraset.2024.58671

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue II Feb 2024- Available at www.ijraset.com

Leveraging Fog Computing, Blockchain, and IoT for Enhanced Healthcare Monitoring Services

Khunaal Aryan[1], Vadlamudi Neel Vittal Bharath[2], Shaik Haji Dowla[3], Shrayanshi[4], Neeraj Sandeep Solanki[5]
[1]B.tech Undergraduate (Information and science engineering), R V College of Engineering, Bengaluru, Karnataka
[2]Project manager in IT-BSG, HDFC bank, Maharashtra, Mumbai
[3]B.tech Undergraduate (Computer science specialization in cyber security), Raghu Engineering College, Visakhapatnam, Andhra Pradesh
[4]Software Engineer - Rapipay Fintech Private Limited, Noida, India
[5]Btech Graduate (Computer Science & Engineering) Maharashtra Institute of Technology World Peace University, Pune , India

Abstract: With the rapid evolution of technology, smart cities have emerged as geographic areas powered by advanced information and communication technologies. These advancements have been significantly influenced by integrating smart technologies, such as the Internet of Things (IoT), blockchain, and fog computing. This paper aims to explore the impact and potential of these technologies on healthcare services within the context of smart cities. Fog computing, as a solution to the challenges faced by integrated Cloud Computing (CC) in IoT applications, offers a promising approach by bringing computation closer to the edge devices. Unlike traditional cloud-based approaches, fog computing enables local data processing and storage, resulting in improved performance, security, and reduced latency. Furthermore, fog computing acts as a middle layer between IoT sensors/devices and cloud data centers, facilitating efficient resource provisioning and service administration. In smart cities, IoT, blockchain, and fog computing are pivotal in enhancing healthcare services. While IoT is widely integrated into healthcare systems, it faces challenges such as cost efficiency, data privacy, and data interoperability. In contrast, blockchain technology offers solutions for safeguarding private data, establishing decentralized databases, and enhancing data interoperability. Fog computing, on the other hand, excels in enabling low-cost remote monitoring, reducing latency, and increasing operational efficiency in healthcare services. By synergizing these technologies, smart cities can revolutionize healthcare delivery, offering efficient, secure, and cost-effective services. This paper provides a comprehensive overview of various computing paradigms, features of fog computing, reference architecture, system algorithms, and challenges, emphasizing their critical role in advancing healthcare services within smart city environments. Through strategic integration and adoption, these technologies can pave the way for a transformative healthcare ecosystem in smart cities, addressing the evolving needs of urban populations.

Keywords: Fog Computing, Internet of Things (IoT), Blockchain, Healthcare Services

I. INTRODUCTION

Fog computing is characterized as a highly virtualized environment that facilitates the distribution of networking, storage, and computational resources between traditional cloud (CC) data centers, typically located at the network edge [1]. Within a fog architecture, multiple edge nodes, often referred to as fog nodes, are present, each with limited processing capabilities and storage capacity. In the fog network, edge devices and various servers, known as cloudlets, collaborate within a shared computing environment situated at the network edge rather than beyond it. This arrangement enables clients to receive real-time responses for latency-sensitive applications [2,3]. While initially coined by Cisco, fog computing has been defined from various perspectives by researchers and industry experts. Yi et al. offer a comprehensive perspective, describing fog computing as a geographically distributed computing framework comprising a diverse array of interconnected heterogeneous computing devices situated at the network edge [4]. These devices collectively provide transmission, storage, and elastic computation capabilities in remote environments to a large user base in proximity [5]. Similarly, the OpenFog Consortium outlines fog computing as a system-level, flat framework that decentralizes storage, resources, computing services, and networking across the entire spectrum from cloud to connected devices [6].

Edge computing furnishes computational capabilities through edge servers or devices situated at the edge. Unlike traditional cloud services, edge computing does not inherently rely on cloud services and instead emphasizes the IoT devices on the device side.

According to a specific study, edge computing involves processing resources or networks situated between cloud data centers and data sources. While intelligent sensors and devices can serve as data sources, edge computing encompasses a broader scope. For instance, a cloudlet or a small data processing center serves as the edge of cloud computing for mobile applications, while the IoT gateway acts as the edge between cloud computing and IoT sensors. Similarly, when a cloud computing application runs on a mobile phone, the mobile phone functions as the edge between the cloud and the application. The primary objective of edge computing is to execute operations closer to where the data is generated. From an edge computing perspective, devices not only store data but also contribute to data transmission and processing [7]. Numerous industries and individuals are increasingly depending on smart devices and computers to manage their daily tasks. These intelligent systems produce data through various applications and sensors, resulting in the consistent generation and storage of large volumes of information by industries. The proliferation of IoT has further contributed to the increase in data generated from various types of sensors. Given the rapid growth in data volume and the limitations of conventional databases in handling diverse forms of structured and unstructured data, there has been significant attention towards big data analytics [8].

The predominant cloud services provided by Cloud Computing (CC) encompass Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), all of which are progressing towards the concept of Everything as a Service (XaaS). However, the vast amount of data generated by millions of sensors, referred to as Big Data, cannot be effectively processed and transmitted to the cloud due to potential latency issues [9]. Moreover, certain IoT applications demand faster processing capabilities than what conventional cloud services currently offer. This challenge can be addressed through Fog Computing, which leverages the processing power of smart devices located near the end-user to facilitate localized networking, processing, and storage capabilities at the edge [10]. The integration of fog computing with IoT aims to minimize data transfer to the cloud for storage, analysis, and processing, thereby enhancing efficiency and performance.

II. LITERATURE REVIEW

As Cloud Computing has evolved, it has ushered in a new era of cloud services including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), which have brought forth various challenges across enterprise, software, and educational sectors [11].

Typically, cloud data centers are geographically centralized and distant from client devices, resulting in latency and real-time delays that degrade service quality, cause network congestion, and introduce roundtrip delays. To address these issues, a novel computing paradigm known as "Edge Computing" has been proposed [12]. The core concept of Edge computing involves establishing a hybrid architecture that integrates peer-to-peer and cloud servers with mobile terminals, aiming to mitigate traffic by performing computations closer to the network's edge. End devices such as mobile phones and smart objects, along with edge devices like switch boxes, bridges, and hotspots, as well as edge servers, collectively possess the necessary capabilities to support computations at the network's edge [13].

However, it's essential to note that the Edge computing paradigm primarily focuses on edge computing and does not directly engage with traditional cloud services like IaaS, PaaS, and SaaS [14].

Furthermore, the emergence of Edge Computing has led to the introduction of additional computing paradigms such as Mobile Edge Computing (MEC) and Mobile Cloud Computing (MCC). MEC emphasizes the deployment of two or three-tier applications within the network alongside mobile devices and modern cellular base stations. This approach enhances network efficiency, content distribution, and application development [15,16,17].

Mobile Cloud Computing (MCC) represents a distinct computing paradigm driven by consumer preferences to execute applications primarily on mobile devices rather than traditional desktop computers [18]. MCC specifically addresses challenges related to application execution time, storage limitations, energy consumption, and resource constraints inherent in mobile environments [19]. However, for critical applications, it is often preferable to execute these tasks outside of handheld devices. In response to this need, MCC offers various computational solutions to offload mobile applications and execute them closer to end consumers [20]. MCC incorporates lightweight mirrored servers known as cloudlets to facilitate this process [21,22].

Yi et al. provide diverse descriptions, applications, and challenges about models of Fog Computing [23]. Baccarelli et al. offer a comprehensive review of the Internet of Everything and the Fog domain, presenting a unified perspective on the convergence of the Internet of Everything and Fog computing [24].

Perera et al. introduce a Fog Computing environment from the viewpoints of both clients and developers, with a focus on applications in smart cities aimed at constructing a robust sensing infrastructure [25].

Hu et al. survey Fog Computing, categorizing frameworks and exploring cutting-edge technologies including storage, data processing, security, transmission, privacy protection, and resource governance [26]. Varshney et al. delve into the Fog, edge, and Cloud Computing ecosystems, examining various dimensions of platform abstractions, application features, and system frameworks [27].

Mouradian et al. present Fog frameworks and algorithms based on six distinct assessment principles: flexibility, interoperability, diversification, federation, Quality of Service (QoS) management, and adaptability [28]. Mahmud et al. propose a classification of Fog Computing based on identified challenges and significant aspects within the field [29].

Like Mobile Edge Computing (MEC) and Mobile Cloud Computing (MCC), Fog computing also facilitates computations at both the edge of the network and the core component side. Core components within the Fog environment include core routers, WAN switches, and regional servers, among others, which are utilized in the infrastructure for computations. This infrastructure enables the seamless integration of numerous IoT devices with Fog computing. Moreover, the components of Fog computing situated at the network edge can be positioned in closer proximity to IoT sensors or devices compared to mobile edge servers and cloudlets. Given that IoT sensors or devices are typically densely distributed and require immediate responses to service requests, this approach allows for the computation and storage of IoT data within the vicinity of these sensors or devices. Consequently, the waiting time for real-time IoT requests to be serviced is significantly reduced.

Unlike Edge Computing, Fog Computing can extend Cloud Computing (CC) services such as SaaS, IaaS, and PaaS to the network edge. These distinctive features position Fog Computing as a well-organized and highly promising solution for IoT compared to other related computing paradigms.

III. METHODOLOGY

Fog Computing in conjunction with the Internet of Things (IoT) addresses various challenges encountered by the current integrated Cloud Computing (CC) framework in IoT applications. Time-sensitive tasks like augmented reality, audiovisual streaming, and gaming are not adequately supported by the existing framework, which lacks responsiveness to location due to its integrated nature. These limitations are mitigated by Fog Computing, which extends processing and storage capabilities, along with cloud network functionality, to the network edge.

This approach effectively addresses the immediate needs of IoT devices and ensures secure and efficient handling of IoT requests. Fog Computing enables the deployment of diverse applications and services across geographically dispersed locations. It facilitates efficient real-time communication among numerous IoT devices, including connected vehicles, among others. Particularly for time-sensitive applications such as augmented reality, audiovisual streaming, and gaming, Fog Computing emerges as a superior option, significantly reducing waiting times.

Integrating IoT with Fog Computing yields several advantages for various IoT applications. Fog Computing facilitates instant communication among IoT devices, thereby reducing waiting times, especially for time-sensitive IoT requests. Additionally, a notable aspect of Fog Computing is its ability to support large-scale sensor networks.

A. Level 1: Physical and Virtual Sensors

Various types of sensors serve as the primary generators of information for Fog Computing. These sensors encompass a wide array of devices, including intelligent homes and appliances, CCTV surveillance systems for traffic monitoring, automated driving vehicles, and humidity and temperature sensors, among others. For instance, in a smart traffic surveillance system, continuous traffic status data from various sensors and devices located along pathways and roadside CCTV cameras is essential for effective traffic signal management.

Anticipating future traffic needs necessitates gathering information from diverse GPS sensors. Moreover, virtual sensors play a crucial role, particularly in scenarios like road accidents. Relying solely on a single physical sensor may not provide sufficient information to make decisions such as whether to block the road or allow traffic to continue.

With multiple lanes and alternative routes impacted differently by the incident, the ability to manage traffic effectively may be compromised. In such cases, virtual sensors can offer immediate solutions for traffic rerouting, lane multiplexing, and assessing road conditions. Therefore, the sensor ecosystem comprises both physical and virtual sensors, with any information-generating device falling into one of these categories.

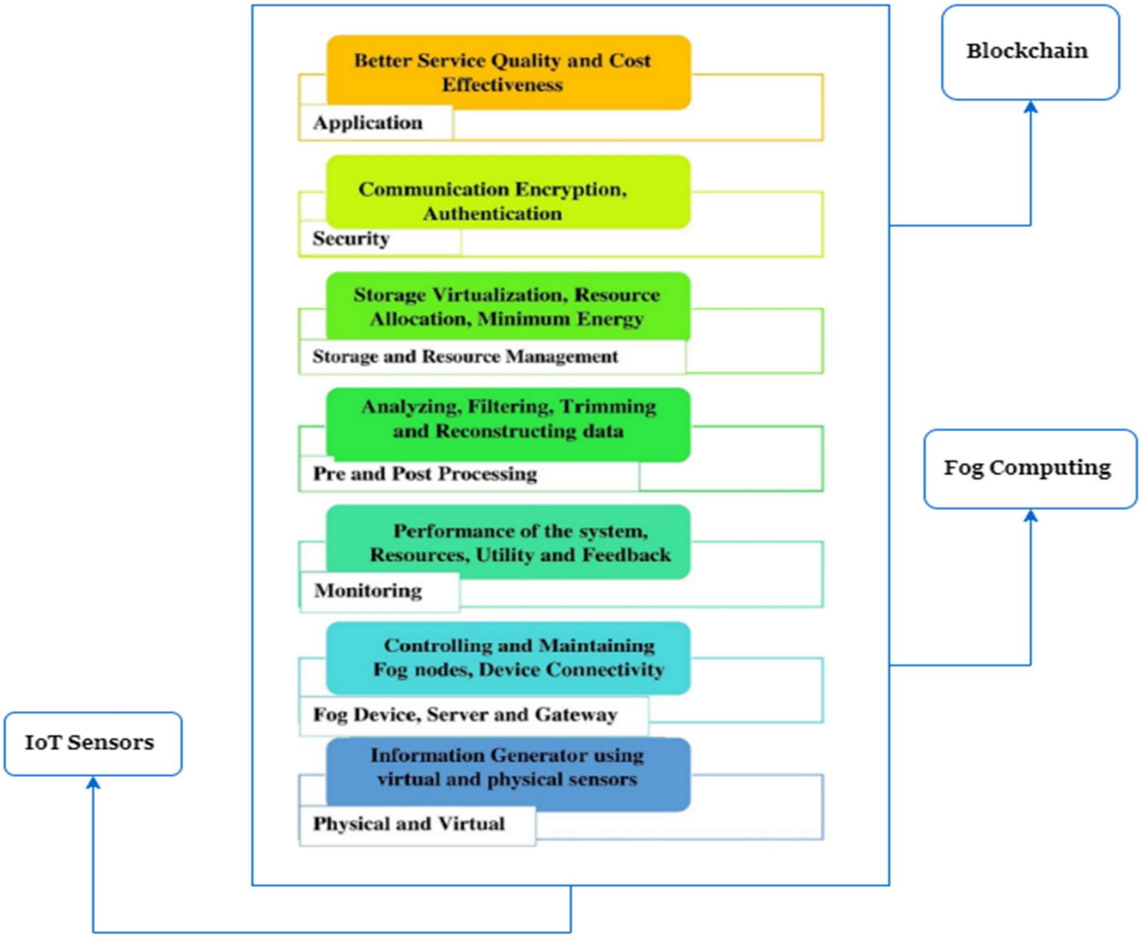

Fig. 1. The proposed framework for BC-FC-IoT Integration

B. Level 2: Fog device, server, and gateway

In the realm of Fog Computing, an IoT device or a standalone device can function as a fog server, fog device, or gateway. However, it is evident that a fog server requires a superior configuration compared to fog gateways and devices due to its management of multiple fog devices, as illustrated in Fig. 1: The proposed framework. Various factors contribute to the operation of a fog server, including hardware configuration, network connectivity, and the range of devices it can oversee. The role of a fog server is determined by its integration with the IoT ecosystem. Clusters comprising virtual and physical sensors are interconnected with fog devices. Similarly, clusters of fog devices are connected to the fog server.

C. Level 3: Monitoring

The monitoring level plays a crucial role in tracking the performance of the system and its resources, while also providing utility and feedback. During system operation, relevant resources are selected for monitoring to ensure optimal performance. In scenarios involving smart transportation systems, various operations are executed, which may require recalibration of resources or storage allocation on fog devices. Similar situations may arise on the server side of the fog infrastructure. To address such scenarios, devices, and servers within the fog ecosystem may seek assistance from other peers. Therefore, the efficiency of these decisions is contingent upon the components of the system monitoring. The resource demand component assesses current resource utilization and forecasts future resource requirements based on user activities and usage patterns. This proactive approach helps mitigate potential risks of system failure. Additionally, the prediction monitor evaluates network load and resource availability to gauge the performance of the fog system. This predictive capability is essential for maintaining the desired Quality of Service (QoS) attributes outlined in Service Level Agreements (SLAs).

D. Level 4: Pre- and post-processing

This level is dedicated to the analysis of both basic and advanced data and comprises multiple components. Its primary function is to acquire data through analysis, filtering, trimming, and reconstructing processes as necessary. Upon processing the data, a component called data flow determines the appropriate storage location, whether locally within the fog or in the cloud for long-term storage. A key challenge in fog computing is minimizing data storage at the edge, emphasizing the transmission of frequently accessed data to fog servers and less frequently accessed or dormant data to the cloud. In the context of smart transportation applications, data is generated from various sensors, which is then explored and processed to extract relevant information.

E. Level 5 Storage and Resource Management

The storage module oversees data storage operations utilizing storage virtualization. Within this module, the data backup component ensures data availability and guards against data loss. Storage virtualization entails a pool of devices responsible for storage within a network, collectively functioning as a single storage entity. This unified storage entity offers easy management and maintenance, thereby reducing hardware and storage costs while enhancing enterprise functionality and minimizing storage complexity. Given the possibility of storage failures, it is imperative to implement data backup mechanisms. The data backup module is tasked with configuring periodic backup schemes to safeguard data integrity. At the resource management level, various components handle resource allocation, scheduling, and energy conservation. The reliability component ensures the dependable scheduling of applications and allocation of resources. During peak resource demand periods, scalability is ensured for fog resources, with cloud platforms primarily achieving horizontal scalability while fog platforms aim for both vertical and horizontal scalability. One critical issue arises in the allocation process within distributed resource systems, particularly concerning storage management across distributed resources.

F. Level 6: Security

The security level is responsible for addressing all security-related concerns, including communication encryption and secure storage of sensitive information. This level ensures the protection of user data within the fog environment. The architecture of the fog environment is conceptualized to function as a utility system akin to a cloud environment. In contrast to the cloud, where users access services directly by connecting to it, in the fog environment, clients connect to the fog system for service access, with middleware in the fog managing and facilitating all communications with the cloud. Therefore, user authorization is essential for accessing services within the fog system. The validation component is tasked with authenticating user requests within the fog environment.

Maintaining security is paramount to prevent intrusion from malicious users, and encryption plays a crucial role in safeguarding communications between different entities. The encryption component ensures that connections between IoT devices and the cloud are encrypted, thereby enhancing security. Given that most fog components are connected via wireless connections, ensuring security becomes even more critical.

G. Level 7: Application

Initially, the concept of fog computing emerged to cater to IoT applications, leading to the integration of fog computing into numerous applications based on Wireless Sensor Networks (WSN). Various applications experiencing latency issues began leveraging the benefits of the fog environment.

This included a wide range of utility services capable of integrating with fog computing to enhance service quality while reducing costs. For instance, applications utilizing Augmented Reality (AR) systems can adopt fog infrastructure, potentially revolutionizing the current technological landscape. The need for real-time processing in AR applications can be effectively met by the fog environment, leading to sustained enhancements across various AR services.

IV. RESULTS & DISCUSSION

Fog computing exhibits adaptability and flexibility in addressing challenges such as resource scarcity and short-term failures. However, the failure of a fog node can lead to system downtime, resulting in the unavailability of resources associated with that node. In the fog environment, these resources are virtualized, presenting several challenges related to resource virtualization, including migration, latency, initialization, and others. Proper management of these challenges is essential to ensure resource availability during periods of downtime.

Let’s discuss Service-oriented computing, Complexity Challenge, Mobilization challenge:

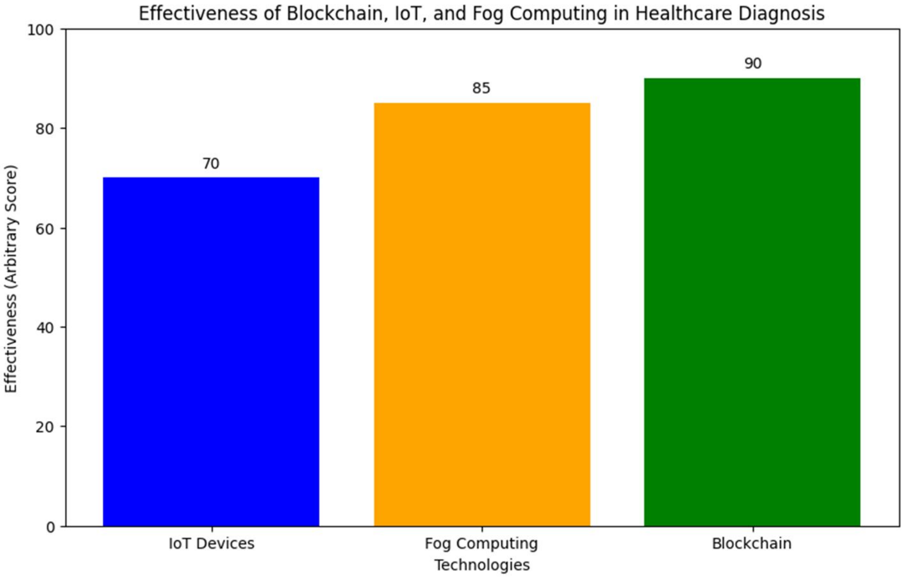

Fig. 2. Arbitrary score of the effectiveness of BC-FC-IoT in Healthcare Diagnosis

In fog computing architecture, client services are segmented into numerous small services, which are then distributed across both cloud and edge environments. This distribution of functionalities over fog devices represents a method of service-oriented computation via edge devices. However, executing small services through fog nodes poses its own set of challenges. The primary challenge lies in organizing the framework effectively to access these services. Small service management encompasses various issues, including service composition, placement, and implementation stages. It is imperative to establish a suitable composition structure to ensure the timely delivery of these services to clients through the fog architecture. In Fog computing, the proliferation of sensors and IoT devices from various manufacturers poses a challenge in selecting the optimal mechanism. This challenge is exacerbated by the diverse hardware structures, software configurations, and individual requirements associated with these devices. Additionally, in certain scenarios where stringent security requirements are paramount, specific protocols and devices may be required to meet the demands of high-security applications. This further complicates the selection process and adds to the complexity of implementation.

Table 1: Experimentation of integrating BC-FC-IoT in a real-world environment.

Device ID	Patient ID	Location	Heart Rate(bpm)	Blood Pressure (mmHg)	Body Temp (C)	Status	Blockchain ID	Fog Computing
HM001	P001	Hospital Room	75	120/80	37.2	Active	0x1aBcDeFgHiJkLm	Enabled
HM002	P002	Home	82	130/85	36.8	Active	0x2bCdEfGhIjKlMn	Enabled
HM003	P003	Nursing Home	68	125/78	37.0	Inactive	0x3cDeFgHiJkLmNo	Disabled
HM004	P004	Clinic	90	140/90	36.5	Active	0x4dEfGhIjKlMnOp	Enabled

Table 1 presents an experimentation of integrating Blockchain (BC), Fog Computing (FC), and Internet of Things (IoT) devices in a real-world healthcare environment. Each row corresponds to a healthcare monitoring device deployed in different locations and monitoring different patients. HM001, located in a hospital room, monitors patient P001. It tracks the patient's heart rate, blood pressure, and body temperature, with a status of "Active."

This device is equipped with Blockchain technology for data integrity and Fog Computing enabled for local data processing. HM002 is deployed in a home environment to monitor patient P002. Like HM001, it records vital signs and has both Blockchain and Fog Computing enabled. HM003 is situated in a nursing home and monitors patient P003. However, it is currently inactive. This device is not utilizing Blockchain technology, and Fog Computing is disabled. HM004 is installed in a clinic setting to monitor patient P004. Like the other devices, it tracks vital signs, has Blockchain enabled for data security, and Fog Computing enabled for local data processing.

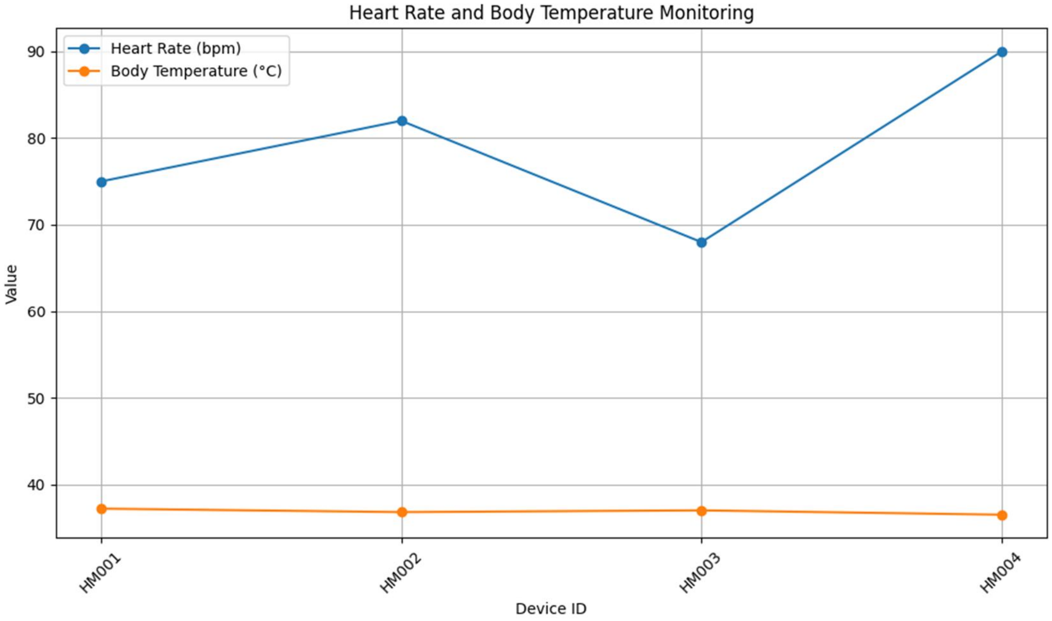

Fig. 3. Heart Rate & Body Temp monitoring

Overall, this experimentation demonstrates the integration of Blockchain, Fog Computing, and IoT devices in real-world healthcare settings to enhance data security, integrity, and local data processing capabilities, ultimately improving patient monitoring and healthcare outcomes. From a Mobilization perspective, OpenFog is characterized as an N-level environment. However, an excessive increase in the number of Fog levels may lead to potential issues in the nascent Fog paradigm. Therefore, it is crucial to establish a definitive number of levels in the case study. Mobilization outcomes will be deemed satisfactory when based on criteria such as the specific tasks performed by each level, the types of sensors utilized, the capabilities of fog devices, and the reliability and latency of fog devices. However, it is imperative to thoroughly assess how these criteria will be met and implemented effectively.

V. CONCLUSION

In the present era, the Internet of Things (IoT) has captured the attention of industries and researchers alike, revolutionizing our lives and becoming indispensable to modern society. IoT has the capability to connect virtually anything in our environment. However, IoT devices often possess limited processing and storage capacities, leading to various challenges within the traditional integrated Cloud Computing (FC) paradigm, including network failures and increased latency. To overcome these challenges, Fog Computing has emerged as an extension of FC, situated closer to IoT devices. In Fog Computing, complete data computation occurs at fog nodes, significantly reducing latency, particularly for critical applications. The integration of IoT with fog computing offers numerous advantages across various IoT applications. This paper presents an overview of different computing paradigms, features of fog computing, and an in-depth architecture of fog computing, including its various levels, along with a detailed analysis of its synergy with IoT. Moreover, it highlights the relevance of IoT, blockchain technology, and fog computing in supporting healthcare initiatives in smart cities. These technologies offer automation of processes and enhance healthcare services, yet challenges remain in streamlining practices, ensuring cost efficiency, maintaining data privacy, and achieving data interoperability. Blockchain technology addresses these challenges by providing highly secure data storage through chained blocks, ensuring data integrity and accessibility only to authorized parties. Similarly, fog computing enhances efficiency in healthcare by enabling low-cost remote monitoring, faster operations, and reduced latency.

In summary, this research aims to explore the integration of fog computing with IoT and address open challenges in this domain. By reviewing current contributions in fog computing and IoT research, this study aims to shed light on upcoming research directions and challenges in this rapidly evolving field.

REFERENCES

[1] F. Bonomi, R. Milito, J. Zhu, S. Addepalli, Fog computing and its role in the internet of things, in: Proceedings of the 2012 ACM First Edition of the MCC Workshop on Mobile Cloud Computing, ACM, 2012, pp. 13–16.
[2] M. Whaiduzzaman, A. Naveed, A. Gani, MobiCoRE: Mobile device-based cloudlet resource enhancement for optimal task response, IEEE Trans. Serv. Comput. (2016).
[3] Y. Chen, Y. Chen, Q. Cao, X. Yang, PacketCloud: A cloudlet-based open platform for in-network services, IEEE Trans. Parallel Distrib. Syst. 27 (4) (2016) 1146–1159.
[4] F. Bonomi, R. Milito, J. Zhu, S. Addepalli, Fog computing and its role in the internet of things, in: Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing-MCC '12, Helsinki, Finland, 17 August 2012, pp. 13–15.
[5] S. Yi, Z. Hao, Z. Qin, Q. Li, Fog computing: Platform and applications, in: Proceedings of the 3rdWorkshop on Hot Topics in Web Systems and Technologies, HotWeb 2015, Washington, DC, USA, 24–25 October 2016, pp. 73–78.
[6] Definition of fog computing, 2018, Available online: https://www.open fogconsortium.org/#definition-of-fogcomputing (accessed on 24 March 2018).
[7] W. Shi, J. Cao, Q. Zhang, Y. Li, L. Xu, Edge computing: Vision and challenges, IEEE Internet Things J. 3 (5) (2016) 637–646.
[8] M.D. Assuncao, R.N. Calheiros, S. Bianchi, M.A.S. Netto, R. Buyya, Big data computing and clouds: Trends and future directions, J. Parallel Distrib. Comput. 79–80 (2015) 3–15.
[9] F. Alhaddadin, W. Liu, J.A. Gutiérrez, A user prole-aware policy-based management framework for greening the cloud, in: Proc. IEEE 4th Int. Conf. Big Data Cloud Comput. (BdCloud), 2014, pp. 682–687.
[10] A.V. Dastjerdi, H. Gupta, R.N. Calheiros, S.K. Ghosh, R. Buyya, Fog computing: Principles, architectures, and applications, in: Internet of Things: Principle.
[11] P. Garcia Lopez, A. Montresor, D. Epema, A. Datta, T. Higashino, A. Iamnitchi, M. Barcellos, P. Felber, E. Riviere, Edge-centric computing: Vision and challenges, ACM SIGCOMM Comput. Commun. Rev. 45 (5) (2015) 37–42.
[12] B. Varghese, N. Wang, S. Barbhuiya, P. Kilpatrick, D.S. Nikolopoulos, Challenges and opportunities in edge computing, in: Proceedings of the IEEE International Conference on Smart Cloud, 2016, pp. 20–26.
[13] W. Shi, J. Cao, Q. Zhang, Y. Li, L. Xu, Edge computing: Vision and challenges, IEEE Internet Things J. 3 (5) (2016) 637–646.
[14] Y.C. Hu, M. Patel, D. Sabella, N. Sprecher, V. Young, Mobile edge computing key technology towards 5g, in: ETSI White Paper 11, 2015.
[15] G.I. Klas, Fog computing and mobile edge cloud gain momentum open fog consortium, ETSI MEC and cloudlets, 2015, Available at http://yucianga.info/?p=938.
[16] E. Cau, M. Corici, P. Bellavista, L. Foschini, G. Carella, A. Edmonds, T.M. Bohnert, Efficient exploitation of mobile edge computing for virtualized 5g in epc architectures, in: 2016. 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2016, pp. 100–109.
[17] A. Ahmed, E. Ahmed, A survey on mobile edge computing, in: The Proceedings of the 10th IEEE International Conference on Intelligent Systems and Control (ISCO 2016), Coimbatore, India, 2016.
[18] M. Othman, S.A. Madani, S.U. Khan, et al., A survey of mobile cloud computing application models, IEEE Commun. Surv. Tutor. 16 (1) (2014) 393–413.
[19] M.R. Mahmud, M. Afrin, M.A. Razzaque, M.M. Hassan, A. Alelaiwi, M. Alrubaian, Maximizing quality of experience through context-aware mobile application scheduling in cloudlet infrastructure, Softw. - Pract. Exp. 46 (11) (2016) 1525–1545, spe.2392.
[20] Z. Sanaei, S. Abolfazli, A. Gani, R. Buyya, Heterogeneity in mobile cloud computing: taxonomy and open challenges, IEEE Commun. Surv. Tutor. 16 (1) (2014) 369–392
[21] P. Bahl, R.Y. Han, L.E. Li, M. Satyanarayanan, Advancing the state of mobile cloud computing, in: Proceedings of the Third ACM Workshop on Mobile Cloud Computing and Services, ACM, 2012, pp. 21–28.
[22] M. Satyanarayanan, G. Lewis, E. Morris, S. Simanta, J. Boleng, K. Ha, Survey and Future Directions Fog Computing: A Taxonomy, The role of cloudlets in hostile environments, IEEE Pervasive Comput. 12 (4) (2013) 40–49.
[23] S. Yi, C. Li, Q. Li, A survey of fog computing: Concepts, applications, and issues, in: Proc. Workshop Mobile Big Data, 2015, pp. 37-42.
[24] E. Baccarelli, P.G.V. Naranjo, M. Scarpiniti, M. Shojafar, J.H. Abawajy, Fog of everything: Energy-efficient networked computing architectures, research challenges, and a case study, IEEE Access 5 (2017) 9882–9910.
[25] C. Perera, Y. Qin, J.C. Estrella, S. Reiff-Marganiec, A.V. Vasilakos, Fog computing for sustainable smart cities: A survey, ACM Comput. Surv. 50 (3) (2017) 32.
[26] P. Hu, S. Dhelim, H. Ning, T. Qiu, Survey on fog computing: Architecture, key technologies, applications and open issues, J. Netw. Comput. Appl. 98 (2017) 27–42.
[27] P. Varshney, Y. Simmhan, Demystifying fog computing: Characterizing architectures, applications, and abstractions, in: Proc. IEEE 1st Int. Conf. Fog Edge Comput. (ICFEC), 2017, pp. 115–124.
[28] C. Mouradian, D. Naboulsi, S. Yangui, R.H. Glitho, M.J. Morrow, P.A. Polakos, A comprehensive survey on fog computing: State-of-the art and research challenges, IEEE Commun. Surv. Tutor. 20 (1) (2018) 416–464.
[29] R. Mahmud, R. Kotagiri, R. Buyya, Fog computing: A taxonomy, survey and future directions, in: Internet of Everything, Springer, Singapore, 2018, pp. 103–130.