A Concurrent Computing Model for Fog Assisted Edge Network Applications

Y. Ameer Hamza[1], Kranthi Kumar[2], Ch Rajini[3], Mahesh Chandrashekar[4]
[1]Lecturer, Engineering Department, College of Engineering and Technology
University of Technology and Applied Sciences, Shinas - Oman
[2]Assistant Professor & HOD, Electrical and Electronics Engineering
Kommuri Pratap Reddy Institute of Technology, Telangana - India
[3]Assistant Professor, Electrical and Electronics Engineering, Kommuri Pratap Reddy Institute of Technology, Telangana - India
[4]Engineering Department, College of Engineering and Technology
University of Technology and Applied Sciences, Shinas - Oman

Article Info

Article history:
Received Jan 4, 2023
Revised Feb 11, 2023
Accepted Feb 26, 2023

Keywords:
Concurrent Processing
Deep Learning
Fog Computing
Network Applications

ABSTRACT

The Fog Computing paradigm is designed to improve the feasibility of service provisioning in the local network applications. This paradigm is proficient in granting services, computations, storage, and communication features for heterogeneous devices. By this consideration, this paper discusses a novel proposal of proliferating computing model (PCM) for improving the robustness in storage level processing. The proposed model makes use of deep learning techniques for improving the concurrency in storage level processing for data storage and access. The learning classifies the functions of requesting and responding devices to improve the rate of data handling along with latency-less processing. This helps to improve the rate of processing by reducing the time along with response rate and less overhead.

Corresponding Author:
Y. Ameer Hamza,
Lecturer, Engineering Department, College of Engineering and Technology
University of Technology and Applied Sciences, Shinas - Oman
Email: ameer.hamza@shct.edu.om

I. INTRODUCTION

Conventional application integration solutions are carried out in a strict and cumbersome process that often requires a lot of time to construct and deploy. These technologies also call for skilled developers and domain specialists. They are server-centric; therefore, they don't fully take advantage of the processing and storage power of client systems, as the Internet's appearance is always changing and new services and innovative apps are appearing and becoming more widely known at an increasing rate.

One of the most talked-about subjects in technology for communication and information is the IoT. Many initiatives have been taken up until this point to integrate and modify IoT with conventional Internet technologies. IoT's goals include identifying devices linked to the Internet and minimizing the need for human intervention in management positions and regulators. Additionally, IoT is expanding the capabilities of the Internet via computers to a variety of objects, digital devices, livestock, and human beings [1], opening up a new paradigm for interactions between human things.

Huge amounts of data are generated as a result of the widespread use of IoT devices. This data needs to be processed and stored, which adds to the network's traffic burden. Furthermore, IoT devices are constrained in terms of computing power, preservation, battery life, and bandwidth (BW), making it impossible to use complicated algorithms on them. IoT technology can help solve many of these restrictions. The IoT and Cloud Computing are combined to create possessions, a powerful cloud-based applications platform that allows for remote device management, tracking, and automation. In below figure 1.1 illustrate the Overview of Concurrent Software Systems.

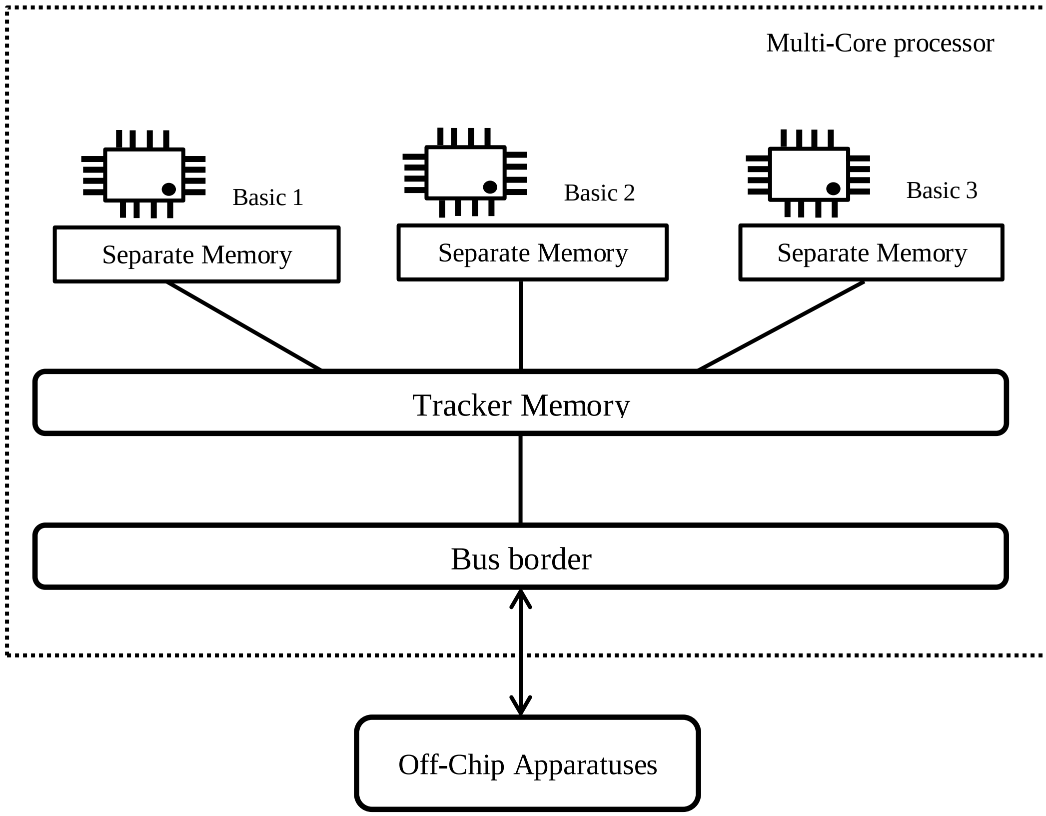

Figure 1.1. Concurrent Software Systems Overview

To enable user tasks to be online whenever and wherever they are needed, the distributed system or cluster of desktops uses the notion of grid computing [2]. But sadly, this brings up the problem of uncertainty in scheduling processes, such as the search function on the Google service, where many users from around the world send their search queries to the Google servers. Search engines use the MapReduce method to divide the requested queries into some specific classifications or groups of tasks and then match these tasks to servers for implementation, which results in three types of unpredictability.

Signal processing and neural network modules that process physiological data are installed in the cloud for conventional telecare systems. In addition, a Fog architecture that used big data analysis and unsupervised machine learning to find patterns in biological information is presented in this book chapter.

So, utilizing fog devices, both spatial and medical data were processed at the edge and then saved in the cloud [3]. The following contributions have been made by the present chapter:

- ➢ It provides the architectural framework and detailed principles for edge, cloud, and fog computers;
- ➢ It talks about the management of services, optimization, safety, and privacy in the context of cloud computing and edge computing.
- ➢ It introduces the idea of big data in the framework of geospatial applications;
- ➢ full deployment of an IoT system with fog assistance for tracking diabetics with cardiovascular illnesses

The list that follows breaks down the essay's main sections. The study on the relevant earlier studies is presented in Section 2. In Section 3, the characteristics of the proposed system and its suggested system are explained using data analysis and the graph-based method. In Section 4, the system's performance is assessed, and the deployment environment is explained. Section 5 presents the outcome.

II. RELATED WORKS

Rahmani, A. M., Gia, T. N., Negash et.al [4] In both industry and research, three-layer architectures with different computational capacities are frequently used for IoT applications. The gateway used in the IoT architecture's intermediary layer serves as the main focus of the majority of associated works. One of many such initiatives is described here, which suggests using gateways to link sensor networks using different protocols, including Ethernet, Bluetooth, and ZigBee, which is also often referred to as the Internet. These gateways can't be altered for various applications, which limits their adaptability. It Presents a gateway named SwissGate that manages and optimizes the operations of a sensor network in a distinct group of related activities.

Simmhan, Y et.al [5] Due to various technological advancements, 2010 is experiencing a similar cyclical transformation, albeit one that is happening more quickly. Along with the explosive growth of smartphones as general-purpose computing devices supported by cloud computing, we have witnessed the implementation of ubiquitous broadband Internet and cellular communication networks, starting with a more centralized cloud computing model providing thousands of Virtual Machines (VMs). Another paradigm made possible by the convergence of various additional technologies is the IoT. To enable vertical IoT areas like personal fitness utilizing wearables, smart utilities employing metering facilities and even self-driving automobiles, sensors and constrained devices linked to the Internet are being implemented.

Muhammad, K., Khan, S., Palade et.al [6] Recently, several clever techniques for enhancing the earlier smoke detection techniques were presented. For instance, analyzed the relationship added a new descriptor called "h-LDS" and described the smoke's texture to increase precision in classification. However, this method has a low detection rate and requires expensive calculation. In the most recent literature, CNN-based smoke recognition techniques has also reported looked into moving images in movies, then watched a CNN to identify smoke. It offers a further method of smoke detection for surveillance networks that incorporates colour and shape information, and it assesses how well it performs on both the CPU and GPU using a CUDA architecture.

Constant, N., Borthakur, D., Abtahi, M et.al [7] The effectiveness of the IoT is growing thanks to more sophisticated sensors, such as body temperature monitors that can detect flu symptoms. Connectivity between wearable technology and home appliances can increase versatility. IoT light sensors could be used to regulate residential lights, among other things. Shortly, it may be interesting to address the privacy risk that may arise while dealing with wIoT-related fingerprints. It concentrated on utilizing a spatiotemporal CNN to learn motion information from video frames for smoke detection. The most recent techniques, which concentrate on shaky video recordings and synthetic smoke images, respectively, are offered based on VGG-16 and multi-scale deep CNN.

Cui, M., Han, D., Wang, J., Li, K. C., & Chang, C et.al [8] Despite the many advantages of cloud storage, there are still certain inherent security risks, including hacker attacks, software system vulnerabilities, and hardware failure. Data owners lose physical authority over the outsourced data because they don't store their data locally, making it impossible for them to know where their information is stored or who has access to it. Additionally, cloud services may remove users' rarely used data to conserve storage space and increase profit. Users' top concern is the security of their data in the cloud, and amid that security, the data's integrity is crucial. Therefore, it is a pressing issue for users to determine the reliability of data that has been farmed.

Yousefpour, A. et.al [9] The most recent assessment examines networking and the setup requirements for fog computing systems and lists critical qualities that they must have the framework for applications in smart cities. They go on to evaluate current strategies that have been put out to address fog computing's difficulties in the construction of smart city infrastructure. Comparatively, the authors concentrate on designing edge computing infrastructure and managing systems to present a thorough and focused survey on the subject. Additionally, they compare several related computing concepts, such as peer-to-peer calculating, mobile grid technology, and mobile crowd calculating, to describe fog and compute at the edge.

Mutlag, A. A., Abd Ghani et.al [10] Fog computing infrastructure can be created using a single fog node or several connected computation nodes. When more computing is necessary, it is possible to add more fog nodes, which can dramatically improve scalability, redundant operation, and flexibility. The aforementioned qualities meet the criteria for applications in healthcare. One may rely on fog computing because of its improved service quality, minimal reaction time, low latency, excellent location understanding, high portability, etc., and the fact that it successfully supports many healthcare applications. Fog nodes, such as smart routers, pathways servers, central stations, etc., cannot, however, satisfy these demands unless their architecture is modified to work with healthcare applications.

III. METHODS AND MATERIALS

The state of fog computing today

The primary studies are divided into four groups in this section: Figure 3.1 illustrates these categories of features of fog computing.

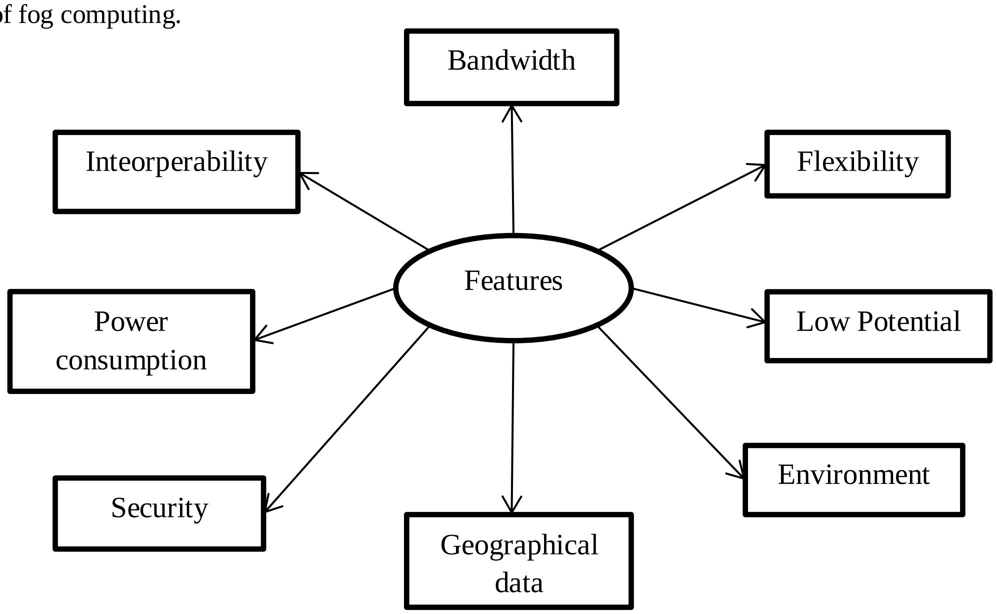

Figure 3.1. The Features of Fog Computing

- **Growth**

The review paper's "growth" section compares the research articles based on their architecture, design sets, approaches, and produced or used algorithms as well as their implementation methods, control, and tracking measures. Additionally, publications that present novel ideas for this group also includes the numerous fog frameworks. The design and structure for fog computing often contain many layers is divided into various groups according to the necessary functions [11]. These structural elements are separated into distinct layers, such as the material layer and the layer for fog sensors, computer systems, and gateways, the layer for monitoring, the layer for storage, the layer for security, the layer for control and managing resources, and the layer for programmers. The important research presenting the idea based on the creation of the fog framework is covered in this subsection.

- **Metrics**

The "Metrics" section evaluates the study based on a variety of performance measures, including latency, dependability, managing resources, reliability, safety, movement, QoS, energy intake, and fog computing framework delivery. The cloud and fog layers use more advanced steps based on complexity and immediate needs. With the aid of the aforementioned techniques, authors have highlighted several specific difficulties in providing security to the populace. Future iterations of this study may involve testing its performance, viability, and applicability through the execution and evaluation of real-world problems and testbeds. In the future, security and ethical concerns can also be addressed.

- **Platforms**

Depending on the tools, applications, and programming languages employed in the research projects, the "Platform" component compares them used to support or develop the fog computing architecture. To compare different research, other aspects such as emulation facility, related storage and networking technology are taken into account. It has also been established that source code accessibility is crucial for future extension. We also go over the summary of significant investigations.

- **Frameworks**

In this section, we've covered several framework categories for fog computing, comprising entity-based, network-driven, event-driven, training simulators, and semi-simulators. The cloud computing architectures are categorized by their communication and operation modes. Additionally, the investigated studies have been divided into three categories depending on the papers' primary foci: academic, industrial, and developmental research.

3.1 Issues with and remedies for real-time services

Numerous IoT requests with low latency are made available to users through fog. If there is no system that works in place to protect users' privacy or maintain their security in IoT apps that utilise fog, real-time services cannot be used comfortably by users due to the world of safety hazards in fog [12]. As a result, learning how to create safe real-time services becomes crucial in fog. In this article, we go over several security issues and propose some innovative solutions.

Identity confirmation:

Real-time services are provided by fog, cloud service breadwinners, and users in several reputable domains. Users' information and IoT services face significant security difficulties as a result of this circumstance because it is difficult to establish trust between all parties involved. Before using these services, each user should be authorized to ensure their reliability and legitimacy. Without enough security assurances, it would be simple for outside attackers to freely target equipment and service assets.

Access Management:

Real-time access credentials to each service are different for various users or IoT devices. When it comes to cloud technology real-time services, a permission architecture is similarly crucial. Anyone can pretend to be an administrator if there is no authorization system in place, giving strong access privileges to regulator both facilities and infrastructures. External attackers would have unrestricted access to user accounts and might interfere with regular services.

Design of Lightweight Protocols:

Fog nodes and IoT devices can connect in one or two hops when using fog computing. Real-time services are made possible by this close-range communication. However, in addition to transmission range and connectivity, the processing postponement on fog nodes also affects the response time. Therefore, the response period will still be lengthy even if the fog nodes need to do complex computational procedures to generate replies for users.

Detecting intrusions:

In fog computing, any entity can be hacked at any time by malevolent external and internal adversaries. If a proper intrusion detection method is not established to identify malicious activity or rule violations on connected devices and fog node networks, the services could be gradually degraded by successful attacks. It is essential to make sure that defense measures are in place to secure the building itself of fog computing.

IV. IMPLEMENTATION AND EXPERIMENTAL RESULTS

The implementation makes use of Google Cloud servers, APIs, and services to maintain, process, and offer cutting-edge services for data. The system's notification push service, for example, is mostly deployed in the cloud [13]. The global websites that may show historical and real-time data in both text and visual format are hosted by cloud servers, much as localhost in fog. End users have a choice of using the worldwide web pages or a PhoneGap-built mobile app that supports both iOS and Android to access data.

The filtered data has, in the majority of cases, a baseline that is distinct from the reference baseline, which is equal to 2 g for acceleration, 1 deg/s for angular velocity, and 0 voltage for the ECG. In order to change the baselines of the signals into the anticipated ones, standard detection and baseline wandering removal are used. Because the identified baseline overlapped for multiple periods, Figure 4.1 does not depict the baseline detection stage.

For determining the baseline of various signals, two alternative methods are used. The baseline of velocity and angular speed must be found, a mean value is used, and for noticing the baseline of ECG, to transform data, a Daubechies d4 wavelet is employed. The processed data are utilized as inputs for algorithms like recognizing falls, heart frequency estimation and QT wavelength extraction demonstrated in Section 4. The amplitude and pattern of the processed data are identical to those of the filtered data.

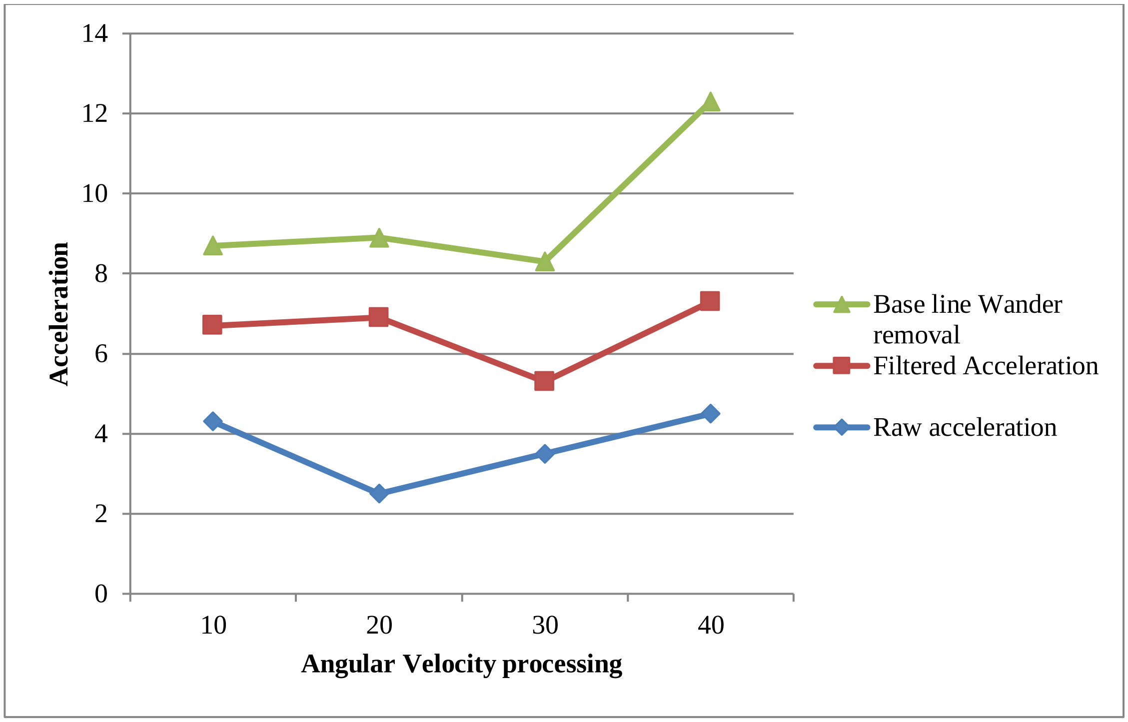

Figure 4.1. Processing of angular velocity and acceleration

The processing of gathered e-health data at fog-assisted smart pathways, which includes acceleration, angular velocity, and ECG, involves three main steps—data filtering, baseline identification, and baseline wander removal—that are illustrated in Figure 4.1. As previously noted, raw data is filtered to remove background noise.

Table 1. Sensor nodes for e-health: combinations and average power draw

Configuration	**Confi-1**	**Confi-2**	**Confi-3**	**Confi-4**	**Confi-5**	**Confi-6**
BME270					Y	
Samples/minute					2	
Insulin sensor						Y
Sample/minute(s)						2
MPU-9260			Y	Y		
Sample/minute(s)			60	60		
AD8330	Y	Y	Y	Y		
Sample/minute(s)	70	140	70	140		
Energy	4.3	4.3	4.3	4.3	4.3	4.3
Present	1.66	4.15	5.58	6.58	0.33	0.46

The experiments examine the power usage of an e-health sensor node in various setups. A sensor node is integrated with a sensor or a collection of sensors in each arrangement. A gateway receives data from the sensor(s) via nRF transmission. Table 1 and Figure 4.2 respectively present comprehensive data on the settings and power consumption statistics. Table 1 shows seven configurations total, with the first three combinations (from Conf 1 to Conf 3) being high statistics rate health sensor node configurations and the last versions (from Conf 4 to Conf 6) being low data rate health sensor node combinations. The final (Conf 6), it supports low- and high-data-rate detectors for hybrid nodes with sensors. According to the findings, high data rate sensors (such as indication sensors and ECG sensors) use a lot of energy while low-speed sensors use very little.

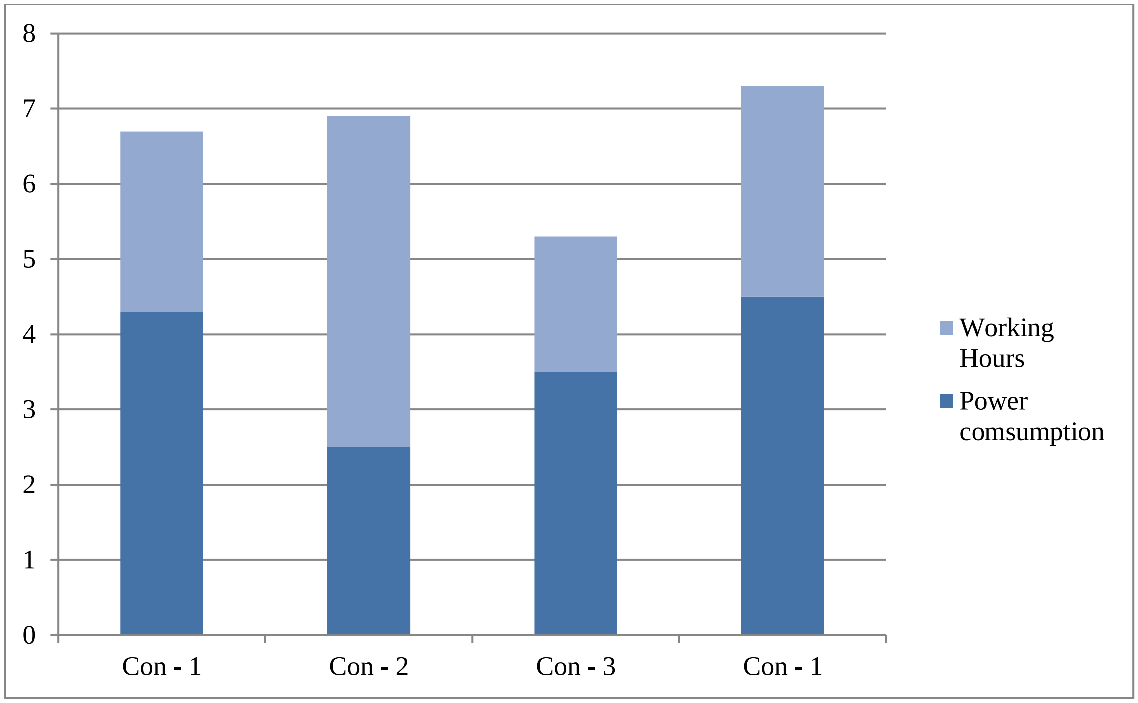

Figure 4.2. Power use for various setups of a digital health node with sensors

According to the findings, high data sensors (such as motion and ECG sensors) use a lot of electricity while low data rate sensors use very little. 2000 mAh Lithium battery, which has dimensions of 61 x 33 x 8, can power the low data rate detector node Con 4 for up to 1640 hours and the high data rate sensing node Configuration 4 for up to 163 hours. About the hybrid sensing node, the same battery may power it for up to 167.5 hours.

V. CONCLUSION

In the context of IoT-based health systems, this study discussed the concepts of fog computing and smart e-health gateways. Smart gateways can take advantage of their beneficial strategic location close to sensor nodes in intelligent home or medical facilities to address a number of difficulties in IoT-based health systems, such as mobility, power consumption, adaptability, interaction, and safety issues. We have examined a variety of high-level services that smart gateways can provide to end users and devices in a distributed manner at the network's edge.

We started by examining the architecture and features of fog computing. Additionally, we discussed the roles played by fog nodes in IoT applications, including real-time offers, temporary storage, data dissemination, and decentralised computation, and we examined a number of exciting IoT projects in the context of these roles. The work's future directions span several fields. The sensor node's battery has a week-long life was already described. With mobile devices in particular, frequent battery replacement is not ideal as it may result in inconvenience, apprehension, and in the case of implanted sensors, agony.

REFERENCES

[1] Khosroabadi, F., *et al.*, "Scatter: Service placement in real-time fog-assisted iot networks," *Journal of Sensor and Actuator Networks*, vol. 10, no. 2, pp. 26, 2021.
[2] Shukur, H., *et al.*, "A state of art survey for concurrent computation and clustering of parallel computing for distributed systems," *Journal of Applied Science and Technology Trends*, vol. 1, no. 4, pp. 148-154, 2020.
[3] Barik, R. K., *et al.*, "Fog assisted cloud computing in era of big data and internet-of-things: systems, architectures, and applications," *Cloud computing for optimization: foundations, applications, and challenges*, pp. 367-394, 2018.
[4] Rahmani, A. M., *et al.*, "Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach," *Future Generation Computer Systems*, vol. 78, pp. 641-658, 2018.
[5] Simmhan, Y, "Big data and fog computing," *arXiv preprint arXiv:1712.09552*, 2017.
[6] Muhammad, K., *et al.*, "Edge intelligence-assisted smoke detection in foggy surveillance environments," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 1067-1075, 2019.

[7] Constant, N., *et al.*, "Fog-assisted wiot: A smart fog gateway for end-to-end analytics in wearable internet of things," *arXiv preprint arXiv:1701.08680*, 2017.
[8] Cui, M., *et al.*, "ARFV: an efficient shared data auditing scheme supporting revocation for fog-assisted vehicular ad-hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15815-15827, 2020.
[9] Yousefpour, A., *et al.*, "All one needs to know about fog computing and related edge computing paradigms: A complete survey," *Journal of Systems Architecture*, vol. 98, pp. 289-330, 2019.
[10] Mutlag, A. A., *et al.*, "Enabling technologies for fog computing in healthcare IoT systems," *Future Generation Computer Systems*, vol. 90, pp. 62-78, 2019.
[11] Singh, J., *et al.*, "Fog computing: A taxonomy, systematic review, current trends and research challenges," *Journal of Parallel and Distributed Computing*, vol. 157, pp. 56-85, 2021.
[12] Ni, J., *et al.*, "Securing fog computing for internet of things applications: Challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 601-628, 2017.
[13] Gia, T. N., *et al.*, "Energy efficient fog-assisted IoT system for monitoring diabetic patients with cardiovascular disease," *Future Generation Computer Systems*, vol. *93*, pp. 198-211, 2019.