An overview of wireless sensor network-based patient health monitoring system

P. Suseendhar[1*]
[1*]Department of Electronics and communication Engineering, Sri ManakulaVinayagar Engineering College, Madagadipet, Puducherry. suseendhar.p@gmail.com
T S Krishnapriya[2]
[2]Department of Electronics and communication Engineering, Sri ManakulaVinayagar Engineering College, Madagadipet, Puducherry.
R.Bavithra[3]
[3]Department of Electronics and communication Engineering, Akshaya College of Engineering And Technology,Coimbatore
Vimal.M[4]
[4]Department of Computer science and Engineering, P.A College of Engineering and Technology,Coimbatore
V.Kavithamani[5]
[5]Assistant Professor, Department of Electronics and Communication Engineering, Jai Shriram Engineering College, Tirupur
Aravindh.G[6]
[6]Department of Electronics and communication Engineering, P.A College of Engineering and Technology, Coimbatore
J.Jaya[7]
[7]Principal,Hindusthan college of Engineering and Technology,Coimbatore

Abstract:
The Internet of medical things (IoMT) is attracting research attention because of its wide range of applications in the healthcare industry. To securely send gathered sensitive healthcare data to the server nodes, smart healthcare sensors, and IoT-enabled medical devices to exchange data and cooperate with other smart devices. Security and privacy concerns make it difficult to safely collect and transmit healthcare data to Fog and cloud servers. IoT applications in the medical sector are examined in this study using a Fog-assisted Secure Healthcare Data Transmission (F-SHDT) system. This system helps raise the level of medical care services in health facilities. This study examines various data collecting and transmission strategies for Fog computing-based systems. Patients will benefit from the study's findings, which point to the potential of IoT in healthcare settings to improve diagnostic accuracy and, in turn, patient care. IoT applications for remote diagnostics will also minimize the frequency of in-person patient visits to the hospital. An application in health facilities will also help provide the right data for the disorders that patients suffer from and therefore use them in scientific study preparation to acquire more accurate findings. This paper presents an Internet-based healthcare monitoring system (HCMS) analysis and a basic outline of prospects and problems for patients' Internet-based healthcare monitoring systems.

Keywords: Fog computing, smart healthcare, monitoring systems, IoT, medical devices, patients

1. Introduction:

An IoT network is a collection of connected smart devices communicating. The development of the Internet of Things (IoT) relies on various intelligent sensory components and wearable smart devices, which play an important role in healthcare, mining, buildings, cities, agriculture, transportation, and industry. Smart medical gadgets, which connect people and things, simplify and ease the healthcare process. In medicine, the Internet of Medical Things (IoMT) is quickly taking over as a critical component. It collects different forms of information and transmits them to cloud repositories to deliver smart healthcare services. IoMT is the thread that holds smart healthcare together.

Consequently, a green solution is needed to address the many challenges in current IoT-based smart healthcare methods. The quality and efficiency of patient medical care can be improved by using medical equipment that allows for remote patient monitoring. Smart collectors or servers near the patient receive health data from patient sensor devices. Patient safety, information organization, and prompt access to crucial health information are all made possible through medical networks. In healthcare, various small devices are used to gather information about patients' medical conditions. There should also be a discussion on the safety of their transmission. Data about a patient's health is sent to the cyber world for processing and analysis in real-time in the context of health monitoring. In this circumstance, improved computer frameworks are needed to dynamically integrate both real and cyber components of medical cyber-physical systems.

Real-time monitoring and feedback control services are termed MCPS in healthcare contexts. An IoT-enabled medical network must be capable of handling complex communication needs and processing a high number of patients. Fog computing designs act as an intermediate layer between the cloud server and the end-user, providing data computing, storage, and networking services. Data aggregation is essential in IoMT to eliminate duplicate patient health factors and lower transmission costs. Various medical sensors are used to gather data in data aggregation. The medical sensor nodes deliver data to the edge devices, aggregating it and sending it to the cloud server. There are two basic kinds of devices used to gather data. Hybrid and homogeneous devices Fog node receives data from devices of either kind.

In Fog-assisted Secure Healthcare Data Transmission (F-SHDT), mobile devices are deployed as collector nodes for effective data aggregation. Nodes in distant health monitoring systems are often placed in hostile environments with insecure transmission mediums, making it a difficult operation. There is the potential for malicious attacks such as data alteration or forgery in such a circumstance. An urgent demand exists for data aggregation that is both safe and private for patients. Protecting the privacy and security of patient data is a top priority on the Internet of Medical Things (IoMT). At both the end node device and the fog node, secure and privacy-protected aggregated data is essential. Because they collect data from sensor nodes and deliver it to the cloud server, edge devices must be authenticated to protect the data's integrity.

Contribution:

Two forms of cryptography are used in data aggregation security techniques. Asymmetric cryptography uses public and private keys to encrypt and decode data securely. The benefit of symmetric cryptography is the ability to encrypt and decrypt data with a single key. The integrity of sensitive healthcare information is dependent on privacy protection and encryption-based security. Data compression has played a crucial role in healthcare data collecting. The compression ratio determines how much data can be compressed into a given space. Decreases communication and processing costs and reduces the time it takes to transfer data to the cloud or edge node.

2. Related work

Priority-based Data Transmission Method (PDTM) for Wearable Sensor-based Healthcare Applications described by Alsiddiky, A. et al [21]. Congestion management and ideal queuing are the selected choice modes that may prevent data losses and reduce the amount of time needed for distribution. Communication is balanced by either queuing or distribution, dependent on the frequency of overcrowding and the priority of the data being sensed, which is described in the decision mode.

IoT-based healthcare information framework (IoT-HIF) using for biomedical applications deliberated by Aktas, F., et al [22]. Nodes and PANc are used to mimic ECG and body temperature signal detection (together with personal information), authentication (through the server), and transmission (via PANc) operations. An updated IoT-based health monitoring and management system may be provided by extending the suggested framework with cloud-based processing and decision-making processes.

Slepian-Wolf-coding-based secret sharing (SW-SSS) for safeguard the confidentiality of patients' personal information illustrated by Luo, E., et al [23]. Patients' information is gathered and stored on many cloud servers as part of the plan. There is no risk to the privacy of patient data, even if one or two data servers are hacked. Several cloud servers work together to supply patients' data to healthcare providers and expose the data's content, which is a patient access control mechanism for healthcare providers.

Fog computing-based smart health monitoring system (FC-SHMS) for wireless communication utilized by Kharel, J., et al [24]. Implementation of a rudimentary testbed for the proposed smart health monitoring system As an IoT-based system, it utilizes the advantages of LoRa wireless communication and fog computing to enhance its performance. The test findings suggest that the proposed system has the potential to transform the clinic-centric health system into a smart patient-centric healthcare system and to provide seamless health services to everyone.

Lightweight User Authentication Scheme (LUAS) for healthcare services expressed by Sharma, G., &Kalra, S. [25].Ensuring the integrity of data and services requires an effective user authentication system. This study outlines a user authentication strategy for remote patient monitoring that was both safe and effective. As a result, the suggested system is able to withstand repeated security breaches and is minimal in weight.The proposed scheme's security has been confirmed by a rigorous verification utilizing the AVISPA tool.

Based on the analysis in the existing method analysis, there are some drawbacks. Hence this paper proposed that F-SHDT visits be reduced due to IoT applications for remote diagnostics. Health institutions may utilize an app to collect data on patient illnesses and use that information in scientific research design to get more precise results.

3. Proposed method:

The growing population and the rising number of patients with chronic illnesses need more attention to disease prevention. Physical activity, a balanced diet, and regular preventative screenings are important components of prevention. It also safeguards against the worsening of existing health issues via long-term management. In reality, the increasing number of chronic illnesses and the lack of medical resources to meet patient care expectations have raised the need for healthcare sector innovation. E-healthcare, or smart/remote healthcare, has

recently been highlighted as a critical component of patient monitoring and diagnosis in the wake of the COVID-19 epidemic.

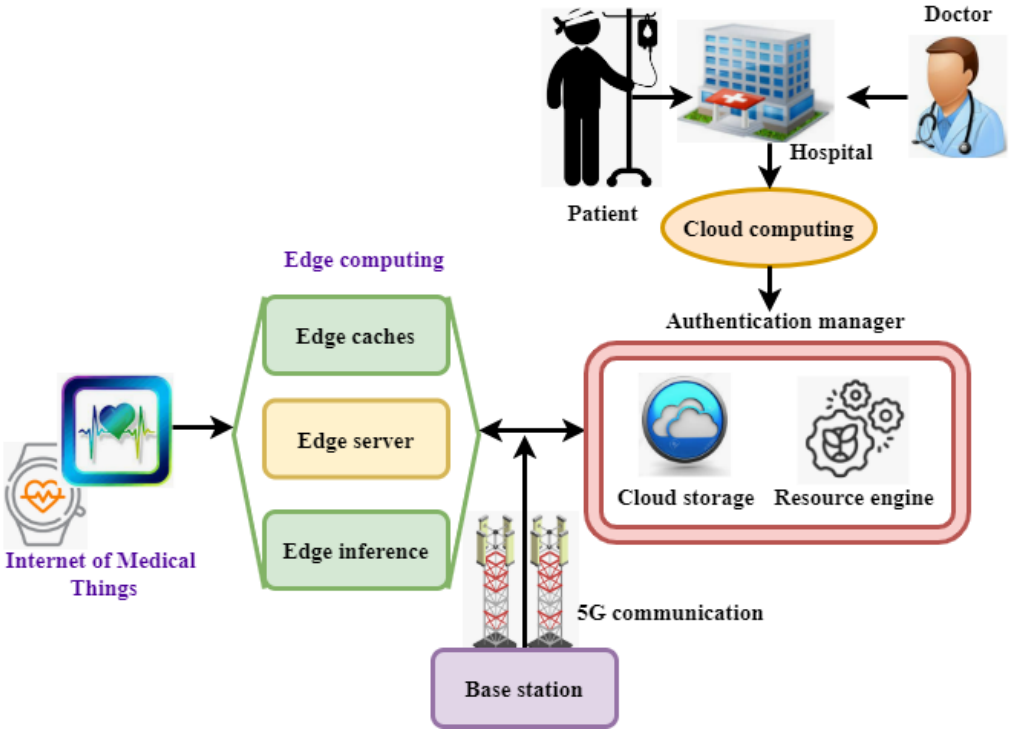

Figure 1: A fundamental model for smart healthcare

Figure 1 shows a fundamental model for smart healthcare. The Internet of Medical Things (IoMT), edge and cloud computing, 4G/5G/6G wireless connectivity, and patients are all shown in Figure 1. The employment of new technologies in safety policies and behavioural structures will benefit the early identification of prospective health concerns and the simultaneous preparation of essential actions, such as treatment monitoring and control or scheduling further tests. Due to AI Edge Inference Computers, a whole new level of computing power is now possible. Intelligence is made possible by AI Edge Inference Computers, which provide real-time inference via hardware acceleration. In the future of computing, intelligent computers will be able to adapt to their environments.

With wearable devices, the Internet of Things (IoT), and wireless communication, smart healthcare systems can connect patients, resources, and organizations to manage their health better and respond to environmental needs. Smart healthcare has many stakeholders, including physicians, patients, clinics, and academic institutions. This intricate system comprises the control and detection of illness, assessment and treatment, healthcare administration, patient decision-making, and medical science. These digital systems include

the Internet of Things (IoT) and sensors; fast Internet; edge and cloud networking; big data; next-generation wireless communication; machine learning; and artificial intelligence (AI).

Sensors are increasingly becoming part of our daily lives because of advancements in computer technology, digital signal processing, and automation. Using sensor data, medical professionals can spot potentially dangerous situations more quickly and precisely, and patients can become more self-aware of their symptoms and changes. Noninvasive technology can help patients and the healthcare business by providing individualized data and digital information. Usage of edge caching refers to the use of cache servers that are located near the end-user. Powerful computers are placed near the network's edge to perform data computations. Physical proximity to the systems or applications that generate the data stored on or utilized by the server is a key advantage of these servers.

In recent years, technological advancements have made it possible to develop monitoring devices that can simultaneously capture multiple physiological signals, such as

- Electrocardiograms (ECGs)
- Blood pressure (BPs)
- Arterial blood pressure (ABPs)
- Electroglottography (EGGs)
- Electroencephalogram (EEG)s
- Electrooculograms (EOGs)
- Electromyograms (EMG)
- Mechanomyograms (MMG)
- Magnetoencephalograms (MEGs)
- Respiration (RESP)

On the other hand, the Internet of Things has increasingly become a part of the healthcare industry's practitioner and patient sides. For example, ultrasonography, BP, glucose sensors, EEG, and ECG devices, among others, are starting to communicate with each other to help patients better maintain their well-being, especially for illnesses that need frequent follow-up visits. Several hospitals have started to deploy smart beds, which detect a patient's movement, dynamically adjust to the proper angle and posture, and provide necessary treatment without needing nurses and caregivers. IoMT refers to the Internet of Medical Things medical equipment. It is expected that the IoMT will play a significant role in creating a fully

integrated healthcare environment. Fitbit, fitness monitors, augmented reality glasses and smartphones are all instances of IoMT.

The structure of IoT and HCMS

This section explains the structure of IoT and HCMS. IoT-based HCMS includes four basic components: IoT medical devices, HCMS information and communication technology (ICT), Internet service (3G/4G), and data management and processing (DMP). IoT and HCMS are shown schematically in Figure 2. The HCMS and IoT components are outlined below.

- **Internet of Things (IoT) Medical Devices**

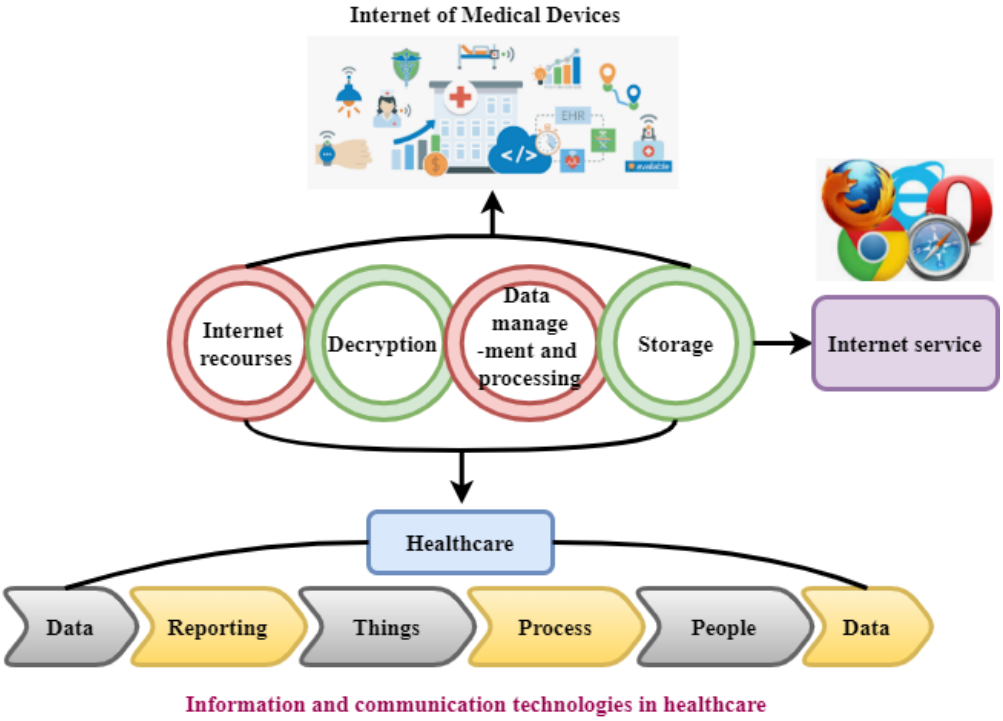

Figure 2: IoT and health monitoring system design

The Internet of medical things is a network of physical devices and embedded systems that interact with electronics, software, sensors, and dynamic actuators that need wireless connections. These devices need a wireless connection to communicate and exchange data. Sensors and actuators that respond dynamically to environmental changes will transform the Internet of Things (IoT). This is an IoT model for HCMS architecture, as shown in Figure 3. The ability to link embedded devices with limited CPU memory and energy resources. It is important to remember that these embedded systems must contain a microcomputer or "microcontroller" to function properly.

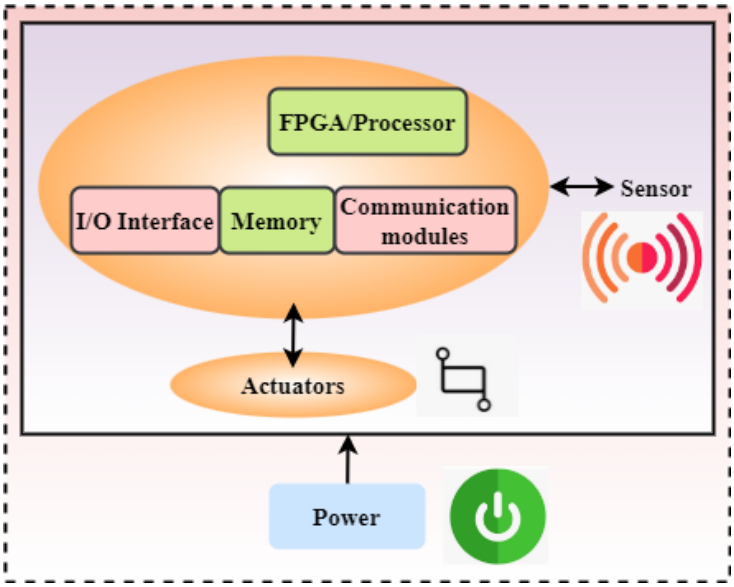

Figure 3: IoT model for the architecture of HCMS

The microcontroller is at the core of the Internet of Things (IoT) platform. These controllers can accommodate various accessories as long as they provide general-purpose input/output (GPIO) capabilities. Medical IoT devices will play the most significant role in IoT systems. These sensors all sense various characteristics, including temperature, pulse/heart rate, muscle, fingerprint, image, pressure, infrared, flow, and strength. They include a thermistor and can be used to track the patient's location. The Internet of Medical Things is already being created through networked medical equipment, healthcare gadgets, and associated applications targeted at improving health monitoring and prevention. Memory, power efficiency, mobility, computational efficiency, coverage, durability, affordability, and dependability are some of the most important advantages of IoT medical devices for HCMS use cases.

An FPGA-based health monitoring system is portable and can continuously monitor health problems using wearable sensors. It may be more cost-effective and easier for medical professionals to monitor patients' health using this new technology. The health monitoring system here makes use of FPGA. When the message is encoded on a physical media, it represents a connection to another system. The observation data is measured using the health monitoring system. The experimental modal analysis is one of the most effective health monitoring techniques using natural frequencies as modal parameters.

- **ICTs in Healthcare Monitoring Systems**

The success of IoT systems in healthcare relies heavily on HCMS's use of information and communication technology. Based on various frequencies, standards, and transmission rates, current information and communication technologies in HCMS are classified. There are two types of communication standards: long-range and short-range. Licensed and unlicensed frequencies make up the spectrum of diverse communication frequencies. Networking, sensor devices, and distribution all have a role in determining data transmission speeds for Internet of Things (IoT) devices.

- **A Web-based service**

Internet access has been facilitated by advances in wireless communications, mobile devices, and services available everywhere. The Internet of Things (IoT) is made up of billions of interconnected devices that communicate with each other through a variety of protocols and IoT middleware, all of which use embedded physical and software components. Structured services architecture is an example of IoT middleware. Connecting to the Internet can be accomplished in many ways: through a smartphone acting as a gateway, a router placed in the house or going straight to the Web server at home. The Internet is the primary network layer that sends data to dispersed computer servers, where it is pooled and analyzed. Mobile phones, computer applications, and programs are usually needed to get the desired results. Internet of Things (IoT) connection allows data to be accessed anywhere, at any time.

- **Data Processing and Management**

Processing and storage capabilities are essential for IoT medical devices to perform fundamental procedures, analyze, and convert measured data. There are a variety of methods by that IoT medical devices can gather and analyze medical data, including directly processing the data or sending it to other devices such as gateways, servers, and cloud applications. The terminal analysis focuses on analyzing data at the network's edge rather than at the centre. Instead of uploading medical data to a cloud server or data centre for processing, the volume of medical data is enormous. Medical data analysis is performed on the same devices or a nearby gateway device (such as a router) directly linked to IoT medical devices. While collecting and sorting through the vast amount of medical data generated, edge-on processing allows one to pick the most critical medical information and send it up.

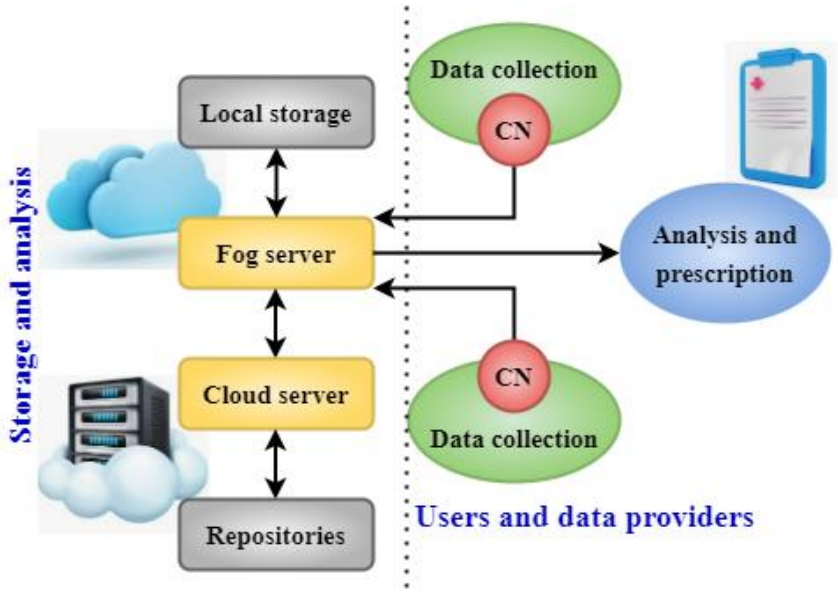

Figure 4: Data aggregation in intelligent medical devices

Figure 4 shows the data aggregative in intelligent medical devices. Sensors are connected to the patient's body to gather information about the patient's health. Data aggregator nodes like smartphones, tablets, and wearable smart gadgets receive this information through sensors. The Fog server receives data from smart collection nodes, including sensitive healthcare information. Patient data is compressed and authenticated in the edge nodes before being stored locally. The fog node converts the data into the format needed by the cloud. When a fog node sends data to the cloud server, the data is stored in the cloud server's repository. Fog servers prioritize transmitting real-time healthcare data to the cloud when the data is not delay-tolerant.

After aggregating data, it is kept in cloud repositories where it is compressed. Authenticated medical personnel and patients may access particular health information stored on cloud servers. The edge node initially receives a request from an authenticated user for the requested information. Edge nodes deliver relevant data to the requesting device if it is available. Otherwise, data is obtained from cloud repositories through edge devices. IoT-based sensing devices may benefit from existing surveys on healthcare data aggregation. In these polls, the transfer of aggregated data is not considered. However, IoT situations were not well examined in terms of security. The secure data gathering and aggregation scenarios were examined; however, fog-assisted approaches were not considered.

Securing data transfer using fog computing, although the drawbacks and difficulties of this approach have not been addressed. Most healthcare-based fog techniques are evaluated for

their usability and usefulness. Fog-based healthcare systems' security is often overlooked in this setting. IoMT security issues, possible remedies, and future concerns are all part of the motivation for this work. Furthermore, it considers the impact of security on the aggregation and transmission of medical information. Researchers are increasingly interested in the fog-assisted strategy because it minimizes data transmission delays while accessing or storing data in cloud repositories.

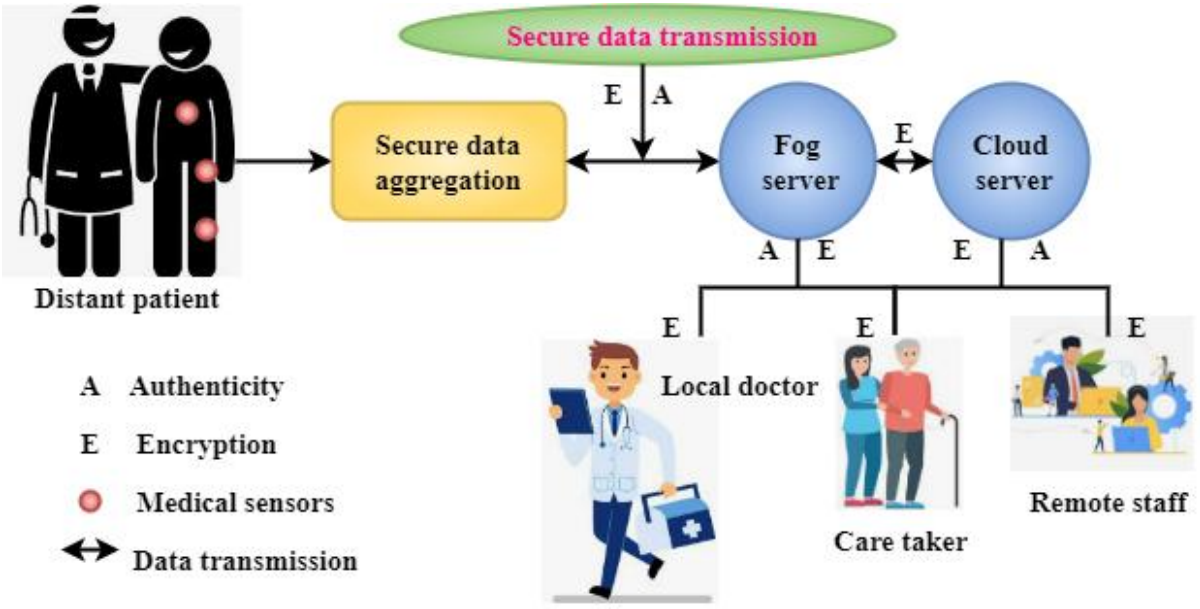

Figure 5: Fog and cloud data transmission and storage are secure

Figure 5 shows that fog and cloud data transmission and storage are secure. As a kind of fog computing in healthcare, the primary goal is to ensure the privacy and security of both local and distant patients' data. Figure 3 illustrates the need for security and privacy while transferring sensitive medical data to the cloud server. A patient-centred healthcare approach reduces the need for clinic-based therapy by allowing medical professionals to follow patients remotely. Generally speaking, a multi-layered framework underpins the patient-centred healthcare system. For example, in this context, fog computing has to deal with various issues, including scalability and latency reduction. Healthcare devices and locally processed data in the fog must be consolidated before being transported to the cloud server.

Fog has developed privacy-preserving healthcare frameworks for electronic medical records (EMRs). In the fog-aided healthcare scenario, the EMR considers privacy to be a major challenge and works on ensuring privacy while maintaining rapid reaction time. Edge devices send data to Fog accumulators, which are processed and analyzed. The identity manager gives patient records a pseudonymous identifier, and the encrypted exchange is initiated for

the devices' safety. Between sensor nodes and a public cloud server, there is a layer known as fog. Because of this, the Fog layer does not need any public cloud server services. A key centre provides a security key in this case.

At the network's edge, Fog-based patient health monitoring systems gather data from various illnesses. Wearable and non-wearable sensors, as well as personal health monitoring software running on edge devices, make up the sensing components of FHMS. Intrinsic and extrinsic sensing data comprise most of the patient's sensitive data. Environmental sensors and biosensors are needed to gather patients' extrinsic data and obtain intrinsic data. Server data is sent to a cloud server and stored there after being processed locally at the fog. A minimal amount of security is provided by utilizing an encryption key, but it does not provide a full security paradigm. Sensing devices may communicate with one another and collector nodes from node to node in the EHDA efficient healthcare data aggregation system. The aggregator node employs a message-reception algorithm to construct a secure aggregate message. Aggregator nodes compress data to decrease energy usage and transmission costs while transferring data to the fog node. The message extraction technique is used at the edge node to retrieve device-level data.

Neighbouring nodes are chosen based on their current load and distance from their neighbours. The current node load will indicate the fog's present condition and whether or not it can take more service requests. While the distance will impact the transfer time and the amount of power needed to discharge the additional weights, the entire round trip delay will be determined by the distance travelled. Fog resource sharing is possible because to a utility model node e_y is unable to process data from things S_y because of the CPU load on e_y and needs a federation with another fog to aid in servicing the requests. This raises the issue, "Which Fog node should e_y couple with?". The neighbouring fog node's power usage is examined using the utility model. To transport data, the amount of power needed depends on the distance between the Fog nodes e_y and e_x, which are willing to exchange resources. As a result, Fn_y^t represents the energy required to transport data from e_y:

$$Fn_y^t(tj, Ct) = \zeta * tj * \left(Fn_{ac} + (CT * Fn_{sa})\right) \quad (1)$$

As shown in equation (1) data transmission rate has been calculated. There is a difference in the amount of energy needed to acquire Fn_{ac} and distribute data, and this difference is known as Fn_{sa}. Whereas, represents the amount of data that can be uploaded at a time ζ and tj is a

amount of data over distance ct. Node consumes energy when receiving data $Fn_y^t(tj, Ct)$is the bandwidth for downloading.

$$Fn_y^t(tj, Ct) = \zeta * tj * Fn_{sa} \quad (2)$$

As calculated in equation (2), energy consumption based on data transmission rate has been described. When transmitting data, node $e_y$uses a data rate ofO_y^t, while receiving it, the node e_y uses a data rate ofO_x^o.

$$O_y^t = \frac{1}{st} * log\ logFn_y^t(tj, ct) \quad (3)$$

As found in equation (3) time slot has been derived. It will be estimated when setting up for various package sizes so that that fog may have the figures of $y$data transformed across $x$distance.

$$O_y^t = \frac{1}{st} * log\ logFn_y^t(tj) \quad (4)$$

As obtained in equation (4), the round trip delay has been computed. It is important to consider the CPU load of fog nodes while picking the optimum node in our system. It will ultimately come down to low CPU utilization, minimal power consumption, and the shortest round trip to create a federation with the best neighbour node.

$$Excecution\ cost = \sum_j^m \quad host(j)(MIPS) \times Sframehost(j) \times costhost(j) \quad (5)$$

Hosts' MIPS (million instructions per second) cost is calculated as the sum of their costs divided by the period. The execution cost is estimated in dollars, computed with the aid of (5). Each host's $MIPS$count $TFrameHost\ time$, and CostHost costs are included in the overall cost of executing a program.

4. Numerical outcome

IoMT attracts researchers' interest because of its vast range of applications in healthcare. Without human involvement, smart healthcare instruments and IoT-enabled medical devices exchange data and cooperate with other connected devices to securely transfer gathered sensitive health information to the system nodes. Securely aggregating and transmitting healthcare data to fog and cloud servers while maintaining privacy and security is a major challenge. Unlike cloud computing for healthcare data exchange, transmission delays may be decreased by using fog computing. Emergency healthcare applications may benefit from this

technology. Investigated are methods based on compressed data collecting that cut data volume and transfer costs by as much as 90%.

i) Security Rate (%)

Medical data stored, shared, and retrieved on the cloud may be protected using a variety of cryptographic approaches. The potential of fog computing technology to keep medical records safe has lately gained interest. Blockchain-based approaches for preserving medical data, either in any form or without fog computing, have been thoroughly investigated in this paper. This project employs blockchain technology to create and evaluate various approaches. Figure 6 illustrates the security rate (%)

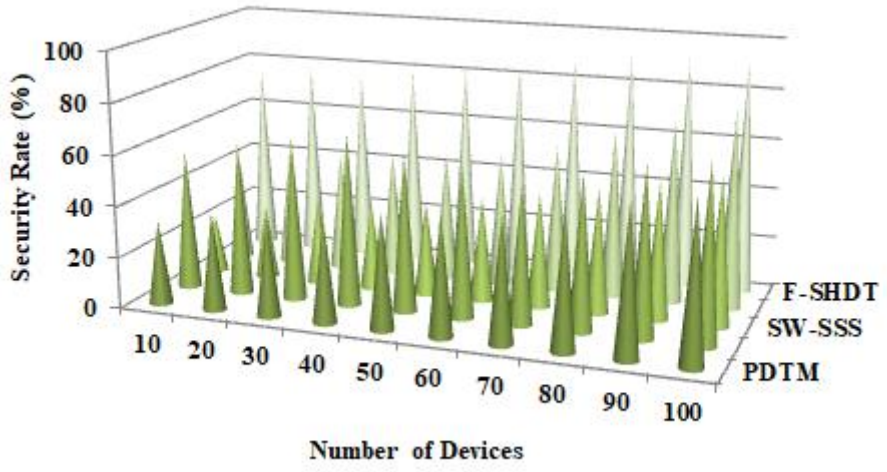

Figure 6: Security rate (%)

Fog computing is incorporated into the decision-making process while diagnosing and treating persons. In addition, they built a consortium blockchain that linked patients, health authorities, institutions, and the pharmaceuticals to establish relations to encrypt sensitive and share medical data.

ii) Performance Ratio (%)

Investor confidence and company success are the most crucial factors for managers to consider when selecting whether or not to adopt machine learning. These algorithms help the company's management make informed choices and implement them. Algorithms based on machine learning may help corporate investors avoid possible dangers by providing vital information. Health, technology, and artificial intelligence work together in the smart

healthcare sector to create a holistic industry. Because it includes all three sectors, this industry has unlimited development potential in the future. All aspects of the smart healthcare industry were examined in our study project. Figure 7 shows the performance ratio (%)

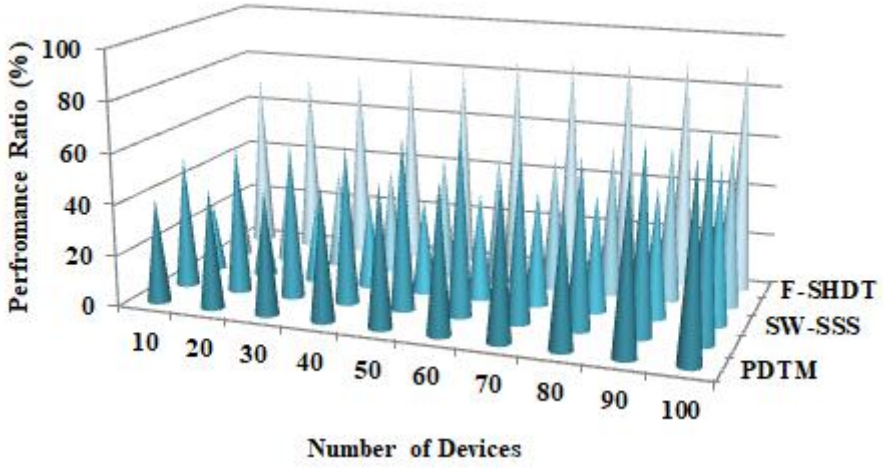

Figure 7: Performance Ratio (%)

$$Performance = Energy_{con} + Execustion_{cost} + Network_{usage} + Network_{delay} + execution_{time} \quad (6)$$

As calculated in equation (6) performance ratio has been described. As a result, the inability to cater to a certain segment of the smart healthcare industry is a huge letdown.

iii) Data transmission rate (%)

fog computing is a paradigm for an intermediate site between cloud computing (data centres) and on-the-ground devices owned by consumers. Fog computing is a scalable cloud computing approach, offering storage and computing near the end. More and more medical computing jobs might benefit from using cloud-based fog computing techniques. Fog can gather, analyze, and store large data, making it possible to conduct real-time analyses while keeping storage and computation costs low. Figure 8 depicts the data transmission rate (%)

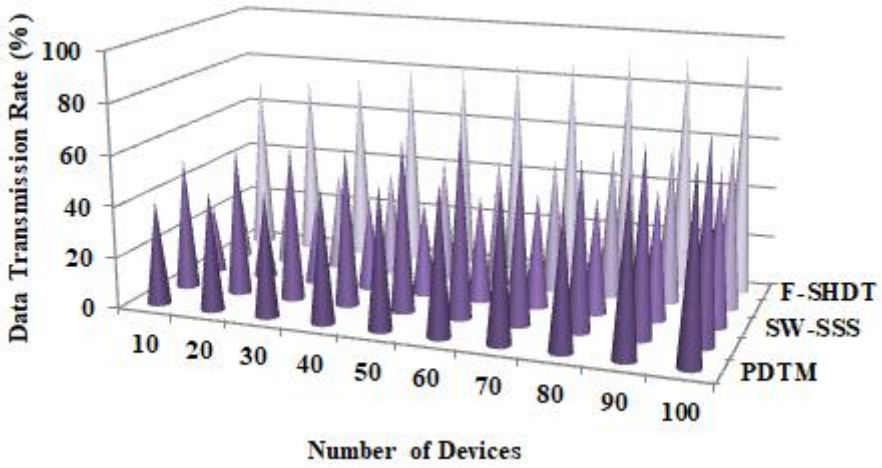

Figure 8: Data transmission rate (%)

Real-time assessment of healthcare sensor data may be enhanced, allowing for intelligent data gathering and decision-making depending on the end-user's local regulations and network resources. As calculated in equation (2), energy consumption based on data transmission rate has been described.

iv) Energy Consumption Analysis (%)

Fog computing is being developed to address the bandwidth, network latency, and energy consumption issues of cloud computing. Like healthcare IoT device management, fog computing has a vital role in fog computing. Massive amounts of data created by healthcare IoT devices must be handled effectively with low latency and failure-free while using the least energy and expense. More delay, maximum energy usage, and high costs may be caused by task or node failures. Well-defined components and stages effectively organize and handle data supplied by healthcare IoT devices. F-SHDT provides a two-way fault-tolerant technique for managing task and node failures, namely task-based and node-based fault tolerance. Figure 9 deliberates the energy consumption ratio.

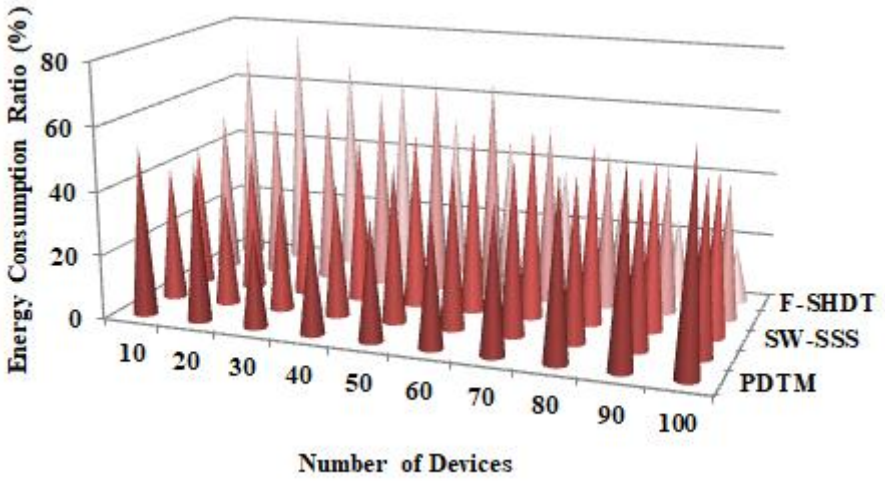

Figure 9: Energy consumption ratio (%)

Because many sensor devices are limited by battery life, energy consumption is an essential consideration for IoT devices. The joule is the unit of energy consumption when an activity requires a specified amount of time to process data (J). During transmission, sensing, and task execution, sensor devices use the most energy. The suggested system's energy usage was determined using (7).

$$Energy\ consumption = \sum_{j=1}^{m} \quad E_{trans\,(j)} + E_{exe\,(j)} + E_{sen\,(j)} \tag{7}$$

As initialised in equation (7), energy consumption has been deliberated. Each activity's energy consumption is broken down into three categories: $E_{trans\,(j)}$, $E_{exe\,(j)}$, and $E_{sen\,(j)}$. Energy cons is the overall amount of energy used, while $E_{trans\,(j)}$, $E_{exe\,(j)}$, and $E_{sen\,(j)}$ are the energy consumption for each individual task.

v) Network Delay (%)

The distance between the IoT smart items and the data centre might make data centre processing infeasible. The amount of time it takes for data to move from the end device to the cloud data centre might impact how useful it is. New "Fog computing" networks are being created to address these concerns. Healthcare systems that rely on the fast processing of sensor data to keep track of patients might benefit from fog computing's ability to increase QoS if it is implemented correctly. This study focuses mostly on healthcare systems. Fog nodes and a cloud data centre are suggested as part of a framework that includes a three-layer architecture. To achieve high quality of service (QoS) in a healthcare system, this framework

provides cooperation across fog nodes with efficient resource management and task distribution. Figure 10 elaborates on the network delay ratio (%)

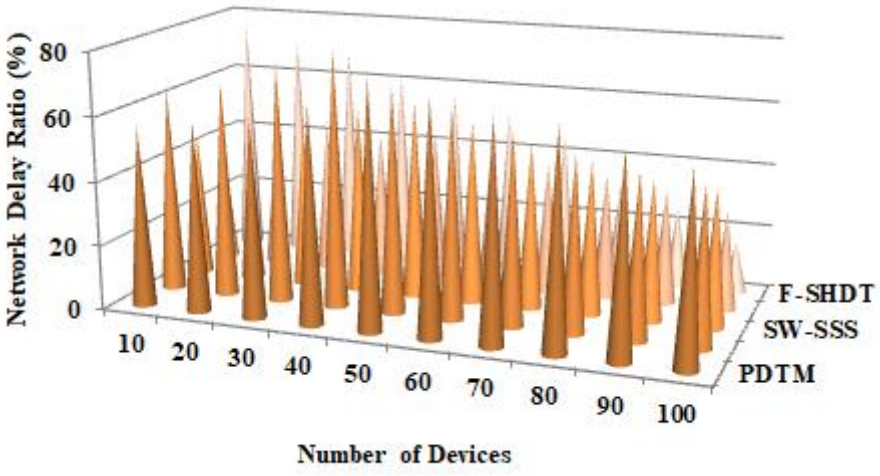

Figure 10: Network Delay Ratio (%)

The network latency is estimated by combining all processing, transmission, and calculation delays. For network delays word "latency" is often used. With the aid of can determine the network latency in milliseconds (ms) (8).

$$Network_{delay} = Q_c + S_c + D_c \quad (8)$$

As demonstrated in equation (8), network delay has been demonstrated. There is a $Network_{delay}$ which represents the network delay, Q_c indicates the transmission delay, S_c indicates the packet delay, and D_c represents the calculation delay.

5. Conclusion with limitation of this research

Many medical facilities aim to improve the standard of care and increase patient satisfaction. One of the finest ways to improve the quality of the services supplied by that institution is via the use of IoT. It may be used in various ways to improve the quality of health care, including acquiring diagnoses and more accurate analyses. By using IoT apps in remote diagnostics, the hospital may save time and money by lowering the number of patient reviews. The second goal is to make it easier for physicians working in healthcare facilities to do practical research since some doctors have difficulty conducting scientific research. The IoT will supply researchers with organized and ready-to-use data. The IoT will motivate medical professionals to conduct studies and research in their areas of expertise. Fog computing with blockchain in healthcare is a solution to many problems, as it is now necessary to retain

patient data and records in an efficient and trustworthy manner as the population expands. Medical records of this size are still a significant problem for fog computing. Authentication and authorization techniques must be strong in healthcare applications since medical data are very sensitive and must be protected from prying eyes. Due to the limited amount of available space in fog, maintaining large amounts of medical information poses an additional difficulty in terms of storage capacity. Cloud-based fog computing for health data management is discussed, as well as its potential benefits and drawbacks for the future of healthcare data management utilizing cloud-based fog computing. The experimental results show the F-SHDT achieve a high-security rate of 93.4%, a performance ratio of 91.5%, a data transmission ratio of 94.8%, an energy consumption ratio of 18.5% and a network delay ratio of 16.3%.

Reference :

1. Tan Q, Xu X, Liang H. Physiological Big Data Mining Through Machine Learning and Wireless Sensor Networks. International Journal of Distributed Systems and Technologies (IJDST). 2023 Jan 18;14(2):1-2.
2. Faris M, Mahmud MN, Salleh MF, Alnoor A. Wireless sensor network security: A recent review based on state-of-the-art works. International Journal of Engineering Business Management. 2023 Feb 8;15:18479790231157220.
3. Chandan RR, Balobaid A, Cherukupalli NL, HL G, Flammini F, Natarajan R. Secure Modern Wireless Communication Network Based on Blockchain Technology. Electronics. 2023 Feb 22;12(5):1095.
4. Rajanna S, Jayaramaiah C, Sridhar R, Chandrappa PH, Venkatesh RT. Fuzzy Inference with Enhanced Convolutional Neural Network Based Classification Framework for Predicting Heart Attack Using Sensor Data. Revue d'IntelligenceArtificielle. 2023 Feb 1;37(1):93.
5. Benkhaddra I, Kumar A, Setitra MA, Hang L. Design and Development of Consensus Activation Function Enabled Neural Network-Based Smart Healthcare Using BIoT. Wireless Personal Communications. 2023 Mar 20:1-26.
6. Khriji L, Bouaafia S, Messaoud S, Ammari AC, Machhout M. Secure Convolutional Neural Network-based Internet-of-Healthcare Applications. IEEE Access. 2023 Apr 12.
7. Arul P, Meenakumari M, Revathi N, Jayaprakash S, Murugan S. Intelligent Power Control Models for the IOT Wearable Devices in BAN Networks. In2023

International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE) 2023 Jan 27 (pp. 820-824). IEEE.

8. Yu S, Yang J, Huang TH, Zhu J, Visco CJ, Hameed F, Stein J, Zhou X, Su H. Artificial neural network-based activities classification, gait phase estimation, and prediction. Annals of Biomedical Engineering. 2023 Jan 21:1-4.
9. Noroznia H, Gandomkar M, Nikoukar J, Aranizadeh A, Mirmozaffari M. A Novel Pipeline Age Evaluation: Considering Overall Condition Index and Neural Network Based on Measured Data. Machine Learning and Knowledge Extraction. 2023 Feb 20;5(1):252-68.
10. Irene DS, Lakshmi M, Kinol AM, Kumar AJ. Improved deep convolutional neural network-based COOT optimization for multimodal disease risk prediction. Neural Computing and Applications. 2023 Jan;35(2):1849-62.
11. García-Cañas Á, Bonfanti-Gris M, Paraíso-Medina S, Martínez-Rus F, Pradíes G. Diagnosis of Interproximal Caries Lesions in Bitewing Radiographs Using a Deep Convolutional Neural Network-Based Software. Caries Research. 2023 Feb 3;56(5-6):503-11.
12. Bhushan TS, Reginald PJ, Krishna MS, Sai NP, Sekar SR. Cluster-Based Techniques in Ad-Hoc Networks for Health Care Monitoring Systems.
13. Samuel S, Ochawar RS, Rukmini MS. Hybrid deep autoencoder network based adaptive cross guided bilateral filter for motion artifacts correction and denoising from MRI. The Imaging Science Journal. 2023 Apr 12:1-6.
14. Sawhney R, Malik A, Sharma S, Narayan V. A comparative assessment of artificial intelligence models used for early prediction and evaluation of chronic kidney disease. Decision Analytics Journal. 2023 Mar 1;6:100169.
15. Swami Durai SK, Duraisamy B, Vinod D, Sathya SS, Shukla SK, Pichandi KV, Qamar S, Muthuchelvi P. Body Sensor Cloud Network Based Data Classification By Machine Learning Techniques In Cognitive Human Computer Interaction.
16. Thirukrishna JT. Certain investigation on healthcare monitoring for enhancing data transmission in WSN. International journal of wireless information networks. 2023 Mar;30(1):103-10.
17. Spyridonos P, Gaitanis G, Likas A, Bassukas ID. A convolutional neural network based system for detection of actinic keratosis in clinical images of cutaneous field cancerization. Biomedical Signal Processing and Control. 2023 Jan 1;79:104059.

18. Kang C, Kim J, Moon H, Chung S. Text Network-Based Method for Measuring Hand Functions in Degenerative Brain Disease Patients. Electronics. 2023 Jan;12(2):340.
19. Warin K, Limprasert W, Suebnukarn S, Paipongna T, Jantana P, Vicharueang S. Maxillofacial fracture detection and classification in computed tomography images using convolutional neural network-based models. Scientific Reports. 2023 Mar 1;13(1):3434.
20. Mori S, Hirai R, Sakata Y, Tachibana Y, Koto M, Ishikawa H. Deep Neural Network-based Synthetic Image Digital Fluoroscopy Using Digitally Reconstructed Tomography.
21. Chauhan NK, Singh K, Kumar A, Kolambakar SB. HDFCN: A Robust Hybrid Deep Network Based on Feature Concatenation for Cervical Cancer Diagnosis on WSI Pap Smear Slides. BioMed Research International. 2023 Apr 17;2023.
22. Cheimaras V, Peladarinos N, Monios N, Daousis S, Papagiakoumos S, Papageorgas P, Piromalis D. Emergency Communication System Based on Wireless LPWAN and SD-WAN Technologies: A Hybrid Approach. Signals. 2023 Apr 30;4(2):315-36.
23. Shrote JN, Pawar JA. SMART AIR POLLUTION MONITORING SYSTEM USING IOT AND RASPBERRY PI.
24. Ma K, Chen H, Lin S. An Ensemble Learning Approach for Exercise Detection in Type 1 Diabetes Patients. arXiv preprint arXiv:2305.10353. 2023 May 11.
25. Neri L, Oberdier MT, van Abeelen KC, Menghini L, Tumarkin E, Tripathi H, Jaipalli S, Orro A, Paolocci N, Gallelli I. Electrocardiogram Monitoring Wearable Devices and Artificial-Intelligence-Enabled Diagnostic Capabilities: A Review. Sensors. 2023;23:4805.