International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

Enhancing Firefly Algorithm for better Network lifetime optimization in Healthcare Monitoring System - Cloud Computing Environment

K. Porkodi[1], Dr. D. Raj Balaji[2]
[1]Research Scholar, Department of Computer Science Rathinam college of Arts and Science,
Coimbatore – 641021.
rheyakodi@gmail.com
[2]Assistant Professor, Department of Computer Science Rathinam college of Arts and Science,
Coimbatore – 641021.
d.rajbalaji@gmail.com

Abstract - The Internet of Things (IoT), a new phenomenon in the technology industry, is mostly responsible for updating healthcare systems by gathering and analyzing patient physiological data through wearable technology and sensor networks. It is difficult to process so much data from so many IoT devices in such a short amount of time. Maximizing the network lifetime is one of the most significant tasks faced by any wireless sensor network. The objective of the study described in this paper was to apply swarm intelligence metaheuristics to optimize the cluster head selection. In order to extend the lifetime of the WSN, we have implemented both the original firefly algorithm (FA) and the proposal for the revised FA. Additionally, According to the proposed study, sensitive data is created and stored by IoT devices, which are vulnerable to attack, and data processing is handled by the edge server. Standard security algorithms like AES, DES, and RSA make it difficult for the majority of IoT devices to function successfully because of their restricted resources. For real-time processing, visualization, and diagnosis, the real-time data is subsequently sent to a distant cloud server.

Keywords: Internet of Things (IOT), Metaheuristics, Cluster head, Network Lifetime, Firefly Algorithm, Cloud Server

I. INTRODUCTION

Over the past decade, the internet and mobile connectivity have completely changed the way people in India consume, which has had a direct impact on business models—including those in the healthcare industry. Access to banking, insurance, transportation, and other services is now easier thanks to digitization and can be obtained almost anywhere. Healthcare access is being impacted by this trend as well [1]. The Internet of Things, or IoT, will help caregivers with equipment tracking, asset management, health monitoring, and more. In addition to helping patients with self-care, connected medical equipment will monitor patients' health. Examples of these devices include smart medicine dispensers. In addition to monitoring, IoT will be used in emergency rooms, patient data transfer, and gamification of health and wellness.

As implantable devices help treat chronic illness, their appeal will increase. In order to give care providers with the information they need to recommend therapy when necessary, they will be utilized to monitor patients' health. Epileptic episodes and other disorders can be predicted by implantable devices as technology develops.

An Internet of Things (IoT) gadget gathers and analyzes data from its environment and user input [2]. Thus, sensors gather information from their surroundings first. The device could consist of a single sensor or a group of sensors. They gather the information, which is then utilized. The GPS, LDR, temperature sensors, and other types of sensors are examples. Subsequently, the sensor sends its gathered data via a connection to the cloud. These connections could be wireless (WiFi), Bluetooth, LAN, satellite, or another type. The application examines and analyzes the data in accordance with the program that exists in it once it reaches the cloud. Usually, this involves using data processing to create forecasts. Data processing examples include reading temperature readings, interpreting weather reports, processing any kind of image, etc. Delivering this data to the client is the most important phase in the process. One way to achieve this is by presenting the processed data to the user in the form of an inference. It also includes updating users about the weather as well as when conditions are expected to rise.

II. IoT

A network of all the smart devices in proximity is connected to the Internet of Things. These devices communicate with one another through sensors and actuators. Actuators react to

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

sensory input, whereas sensors identify movement in the surrounding environment [3]. Gadgets include things like Smartphone's, smart dishwashers, smart TVs, and smart cars.

Think of an Internet-connected pair of smart sneakers. It has the ability to monitor the number of steps it can take. The Smartphone has the ability to read this information and access the Internet. After analyzing the data, it gives the user additional fitness advice along with the energy used.

One tool that can monitor traffic and accidents is a smart traffic camera. Information is transmitted to the gateway via it [4]. This gateway can receive data from this camera as well as other cameras that are similar. Together, these networked devices create an effective system for managing traffic. It distributes, processes, and analyzes data over the cloud. When an accident occurs, the system assesses the damage and suggests actions for drivers to assist in preventing the collision. Internet of Things is, at its core, a new technology that will grow rapidly in the coming years. In addition, there are lots of examples in the industry, healthcare, agriculture, and other sectors. The fact that privacy and safety issues could arise despite the devices' daily data collection is one drawback.

The primary objective of deploying a large number of randomly placed sensors is to locate them as close to the target location as feasible while still providing adequate detection. Deployment can be managed in certain situations, and it's critical to guarantee maximum coverage [5]. Sensor nodes that are deployed must function independently with minimal energy and resource availability, be unsure of their precise locations, and use wireless communication to maintain the longest network lifetime possible. Data transfers throughout the entire network may cease if the critical sensor nodes at the optimal places for the network's routing are exhausted.

III. ROLE OF CLOUD COMPUTING IN IOT

IoT data is stored in a collaborative environment by a cloud computing system. All of the computer resources are stored on a server, which is accessible at all times. IoT-generated internet data packets flow through cloud computing with ease.

Facilitates remote computing The Internet of Things' vast storage capacity makes it unnecessary to rely on on-site infrastructure. The ongoing advancement of internet-based technology, including the internet and gadgets that enable cutting-edge cloud solutions, is the cause of why it has become main stream.

A secure and private environment Utilizing cloud computing and IoT to automate operations, businesses may significantly lower security risks. Additionally, it offers robust security mechanisms for clients through efficient authentication and encryption methods.

Coordinated data administration IoT and cloud integration are made possible by modern technology, which also enables real-time networking and communication. This makes it possible to gather data in real time, integrate data in real time, and analyze important business processes in real time, all while maintaining 24/7 connectivity.

Operational continuity A cloud service makes use of a network of data servers spread across several different countries to keep numerous backup copies of data. In an emergency, cloud computing makes it simple to get data from IoT-based activities.

IV. MAJOR COMPONENTS OF IOT (INTERNET OF THINGS)

The Internet of Things (IoT) is made up of five main parts: devices or sensors, gateways, clouds, analytics, and user interface.

Devices or Sensors

The basic functions of sensors and devices include data collection, transmission, and action execution depending on data. The sensors can be used, for instance, to measure humidity and temperature. There are various kinds of sensors; the following are some of them: The following sensors are available: light, motion, pressure, gas, temperature, humidity, proximity, motion, and GPS.

Entry Point

Another part of the gadget that essentially serves as a middleman between the sensors and the central cloud is the gateway. One of the key elements of the Internet of Things, the gateway the following is a few of the IoT gateway's functions: Protocol translation, load balancing, data aggregation, communication, security, and latency reduction.

The cloud

In the context of IoT, "cloud" refers to the service that offers data management, processing, and storage for devices connected to the Internet of Things. The following are some crucial IoT cloud features: Cost-effectiveness, connectivity, security, integration, and data storage and collection.

Analyses

The key to utilizing the full potential of IoT is this component. Analytics is the analysis of significant information produced by sensors and IoT devices. Analytics encompasses a number of tasks, including statistical analysis, machine learning, and data processing.. Applications of analytics in the Internet of Things include energy management, smart cities, anomaly detection, environmental monitoring, and agriculture.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

Interface with the user

The Internet of Things (IoT) uses user interface, or UI, to refer to the interface that allows users to communicate with systems and applications. The Internet of Things' (IoT) user interface has the following salient features: User-friendly design, security, integration, remote management, personalization, and data visualization.

V. IOT IN HEALTHCARE SECTOR

Prior to the Internet of Things, healthcare providers and patients were able to interact through text messages and appointments in person. A healthcare provider or hospital could not possibly keep an ongoing monitor of their patient's health and make suggestions based on such information [6].

Devices with Internet of Things (IoT) capabilities have enabled remote monitoring in the healthcare industry, unlocking the potential to maintain patients' safety and health and enabling doctors to provide exceptional treatment. Due to the convenience and efficiency of interactions with clinicians, it has also enhanced patient involvement and satisfaction [7]. Reducing the duration of hospital stays and avoiding re-admissions are further benefits of remote patient monitoring. IoT also has a big influence on improving treatment outcomes and drastically lowering healthcare expenses.

Without a doubt, the Internet of Things is revolutionizing the healthcare sector by altering the way that devices and people interact when providing healthcare solutions. Applications of IoT in healthcare benefit doctors, hospitals, insurance companies, families, and patients.

Internet of Things for Patients Patients can receive individualized care through wearable technology, such as fitness bands, and other wirelessly connected devices, such as glucose meters, blood pressure and heart rate monitoring cuffs, etc. These gadgets can be programmed to remember blood pressure fluctuations, appointments, workout logs, calorie counts, and a host of other things [8].

IoT has improved people's lives by making it possible to continuously monitor medical conditions, especially for older patients. This has a significant effect on single persons and their families.

The alert system notifies concerned medical professionals and family members of any disruption or change in an individual's usual activities. Figure 1 shows the four key components of an Internet of Things (IoT)-based health care monitoring system: Internet service, Internet-based medical data processing and administration, Internet-connected medical devices, and information and communication technologies in HCMS.

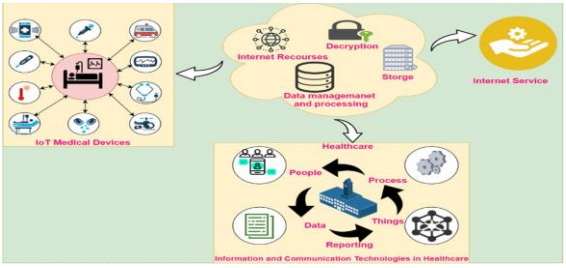

Figure 1: Illustration of IoT and healthcare monitoring system

IoT for Doctors: Doctors can better monitor their patients' health by employing wearables and other IoT-enabled home monitoring devices. They can monitor whether patients are following their treatment regimens and whether they require emergency care. Proactive patient communication and increased vigilance are made possible by IoT for healthcare workers. Physicians may determine the most effective treatment plan for their patients and achieve the desired results with the use of data gathered from IoT devices.

IoT for Hospitals: In addition to keeping track of patients' health, IoT devices have numerous other applications in medical facilities. Sensor-tagged Internet of Things (IoT) devices are used to track the real-time position of medical equipment, such as oxygen pumps, defibrillators, wheelchairs, and nebulizers. Real-time analysis is also possible with regard to the medical staff's deployment at various locations.

For patients in hospitals, the spread of infections is a serious problem. IoT-enabled hygiene monitoring tools assist in keeping patients from contracting infections [9]. IoT devices are also useful for asset management, such as controlling pharmaceutical inventories and monitoring the environment by controlling humidity and temperature as well as checking the temperature in refrigerators.

Health Insurance Companies and IoT - Health insurers can benefit greatly from IoT-connected intelligent gadgets. Health monitoring device data can be utilized by insurance firms for underwriting and claims processing. Organizations will be able to identify individuals for underwriting and detect fraud claims according to this data. IoT devices increase availability in underwriting, pricing, claims processing, and risk assessment process between insurers and clients. Users will be provided with adequate insight into the underlying reasoning behind each decision made and process outcome in the context of IoT-captured data-driven decisions in all operation processes.

Customers of insurers may receive rewards for utilizing and disclosing health information produced by Internet of Things devices. Users using IoT devices to monitor

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

their regular activities, adherence to treatment regimens, and preventive health measures might receive rewards from them [10]. This will greatly aid insurers in lowering claims. Insurance firms may be able to verify claims with IoT devices by using the data these devices collect.

Redefining Healthcare

The proliferation of healthcare-specific IoT products opens up immense opportunities. And the huge amount of data generated by these connected devices holds the potential to transform healthcare.

IoT has a four-step architecture that is stages in a process (See Figure 2). All four stages are connected in a manner that data is captured or processed at one stage and yield the value to the next stage. An integrated value in the process brings intuition and delivers dynamic business prospects.

Step 1: The first step consists of the deployment of interconnected devices that include sensors, actuators, monitors, detectors, camera systems, etc. These devices collect the data.

Step 2: Analog data from sensors and other devices is typically received in this form; for additional data processing, this analog data must be combined and converted to digital form.

Step 3: The data is pre-processed, standardized, and transferred to the data center or cloud after it has been digitalized and aggregated.

Step 4: Final data is organized and examined to the necessary extent. When advanced analytics are used on this data, useful business insights are obtained that help in decision-making.

In the healthcare sector, IoT is revolutionizing things like treatment outcomes, cost, workflows, and patient experiences for medical personnel, just to mention several things.

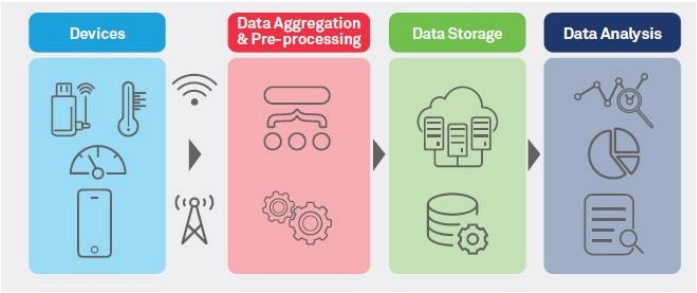

Figure 2: The four stages of IoT solutions

THE MAJOR ADVANTAGES OF IOT IN HEALTHCARE INCLUDE:

Cost reduction: Real-time patient monitoring made possible by IoT greatly reduces needless doctor visits, hospital stays, and readmissions.

Enhanced Care: It provides complete transparency and empowers doctors to make evidence-based decisions.

Rapider Illness Diagnosis: Based on symptoms, real-time data and ongoing patient monitoring assist in the early detection of diseases.

Proactive Medical Care: Ongoing health monitoring makes it possible to provide medical care that is proactive.

Drug and Equipment Management: In the healthcare sector, managing pharmaceuticals and medical equipment presents significant challenges. These are effectively controlled and used at a lower cost thanks to connected devices.

Error reduction: Information produced by Internet of Things (IoT) devices not only facilitates efficient decision-making but also guarantees error-, waste-, and system-free healthcare operations.

IOT APPLICATIONS IN HEALTHCARE

The healthcare Internet of Things (IoT) market is expected to develop at a compound annual growth rate (CAGR) of 37.6 percent between 2015 and 2020, based on studies given by P&S Market Research. One thing is for sure: over the past several years, IoT has significantly changed healthcare and will do so for years to come. Figure 3 illustrates how IoT is being used in the healthcare sector.

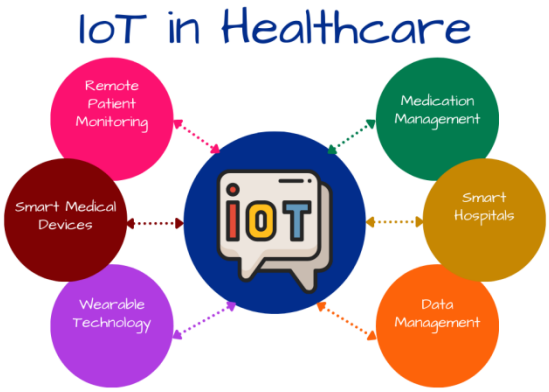

Figure 3: Application of IOT in Healthcare System

Glucose Monitoring Systems Implanted

Individuals with diabetes may be able to have devices with sensors inserted under their skin. When a patient's blood sugar falls too low, the sensors in the gadgets will notify them via text message on their phone and store past data for them as well. Patients will be able to determine when they are most likely to experience low blood sugar levels both now and in the future.

Activity Monitors for Cancer Patients

A cancer patient's age and weight are not always the only factors that determine which treatment is best for them

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

Their fitness levels and habits also have a significant impact on the type of treatment that is best for them. Activity trackers monitor a patient's eating, sleep patterns, and level of weariness. Additionally, the information gathered from the tracker both before and after therapy begins will help medical professionals determine what modifications should be made to the suggested treatment plan.

Heart Rate Trackers with Reports

Individuals with high blood pressure can be identified by wearing gadgets that track their heart rates. When they need to pull patient cardiac monitor data for examinations and checkups, medical professionals will have access to it. Healthcare providers can receive alerts from the wearable devices in the event that a patient has a heart attack, palpitations, arrhythmia, or stroke. The quick dispatch of ambulances can therefore be the difference between life and death.

Systems for Medical Alerts

People might wear items that resemble jewelry but are made to notify friends or family in the event of an emergency. For example, in the event that a person wearing a medical alert bracelet falls out of bed in the middle of the night, their designated emergency contacts will be alerted quickly via smart phone of the need for assistance.

Multifunction Sensors

Devices with sensors that resemble tablets can now be swallowed by patients. The sensors provide data to a patient's smart phone app, which enables them to adhere to the recommended dosages for their drugs, as soon as they are used. The majority of pharmaceuticals aren't taken as directed because of human error or forgetfulness. The purpose of this edible sensor is to guarantee that patients are taking the appropriate drugs at the appropriate times and quantities. Additionally, certain ingestible sensors are being used to diagnose individuals with conditions like colon cancer and irritable bowel syndrome more precisely.

Pharmacological Dispensers

Patients can now have devices implanted that deliver consistent dosages of medication all day long. When it's time for patients to refill their prescriptions, they will be informed. Missed doses can also be reported to doctors at routine checkups.

Connected Wireless Sensors

To guarantee that blood samples, cold pharmaceuticals, and other biological materials are constantly kept at the right temperatures, wireless sensors are being employed in labs and hospital freezers.

Traceable Inhalers

By sending data to patients' cell phones or tablets, IoT inhalers can tell patients what triggers an asthma attack. Their doctors can also be informed of this information. Patients are also reminded to take their prescriptions on time via the connected inhalers.

Wearable Technology to Avoid Depression

Software developed by Apple for the Apple Watch aids manic-depressive individuals in managing their depression. The app monitors mood and cognitive functioning and keeps track of a patient's episodes that occur outside of regularly scheduled appointments.

Pairing Contact Lenses

Patients with diabetes can now have their glucose levels read by connected contact lenses. However, they will eventually be able to assist in regaining the eye's focus and enhancing vision.

Place-Based Services

Medical staff may find and tag items such as wheelchairs, scales, defibrillators, nebulizers, pumps, and monitoring equipment with IoT sensors. IoT will allow personnel to know where everything is, unlike physical equipment that is frequently lost or difficult to find.

Remote Sensing

Healthcare providers can use Internet of Things (IoT) devices to keep an eye on their surgical or outpatient patients after they return home. If a patient enters a serious condition or requires emergency care, they will be notified.

VI. LITERATURE REVIEW

In 11, the author Snehal Sanjay Kale target the security required in BSN based present day medicinal services framework. And also invent to protected IoT based human services framework utilizing BSN, called BSN-Care, which can ensure to effectively finish those prerequisites. Accordingly, whatever is left of the article is sorted out as takes after. Secondly, we introduce a rundown of security parameters which are need to be tended to in any IoT based social insurance framework utilizing BSN. Thirdly, we depict a portion of the associated works in IoT based human services framework utilizing BSN. At last, we presented our BSN-Care framework and thusly, in this segment, we likewise so demonstrate to implement security in our BSNCare model to accomplish all the fundamental security properties.

In 12, the author Ala Saleh Alluhaidan illustrated to distinct EEG signal data sets are used as a source of data for encryption and decryption. Before being delivered to the hybrid lightweight encryption technique, the data are

preprocessed (transformed Paillier and KLEIN algorithm). Transformed Paillier is key pair based cryptography that adds homomorphism to the system. Because messages are encoded and will interpret as needed, they may be merged in this manner. Every client is given a private and public key, and messages encrypted with the public key may be decoded with the private key. KLEIN is a lightweight encryption estimator that is impacted by key space; it utilizes the EHO improvement framework to minimize key space. #is decreases the degree of a cycle and, as a result, the amount of space available. Finally, the EEG signal data have been encoded and unscrambled.

In 13, Abdulmohsen Almalawi et.al proposed design of security management in smart healthcare management is illustrated in Figure 1. The COVID data were collected locally and globally by IoT-based sensors, which was helpful for electronic medical records administration. The serpent (S) encryption technique based on LRO to protect data transfer from sensed data was applied. The LRO algorithm created the secure key for the serpent algorithm. The wearable IoT device stored its acquired data on a cloud server and was open to hacker attacks and privacy violations from unauthorized users. The asymmetric hash signature function was validated in the intelligent healthcare management system for critical validations from the sender and receiver. If both perform the same position, only the secret key was sent to the recipient, who may then use it to decode the data. A similar process was used for hospital-based medical professionals.

In 14, the author Kirtirajsinh Zala et al, proposed Key Conclusion Function (KCF) technology to the hospital for monitoring all patients' health and their data is to be stored securely in cloud. The solution we provided was for medical records to be stored in the cloud, saving hospital staff time and effort by eliminating the need to manually enter data.

In 15, the author Khalid K. Almuzaini encrypted data structure of medical and healthcare prescriptions is recorded as they move through the hands of patients and healthcare facilities, according to the technique recommended. The double encryption approach is used in order to raise the overall degree of security. An encryption class is created by referring to the Ciphertext ID during the encryption procedure. The key holder is a master secret key that facilitates in the recovery of the secret keys of various monsters and creatures by acting as a conduit between them. It is transferred and stored as a single aggregate for the benefit of the patient or customer in order to make decryption more convenient and efficient. A safe connection between cloud-based intelligent health monitoring systems and healthcare organizations and their patients may be established via the use of a key aggregation cryptosystem and a double encryption approach, according to the researchers. Because of this, when compared to earlier techniques, the findings reveal that the research methodology provides high levels of security in terms of confidentiality and integrity, in addition to excellent scalability.

In 16, the author A. Pugazhenthi describes however this problem can be resolved in proposed method since it introduces sharing of the data securely using a method called Improved Diffie Hellman Key Exchange Algorithm (IDHKE). By introducing the Improved Diffie Hellman Key Exchange Algorithm, securely sharing the secret keys to the receivers of the data has been achieved. The secret key details can be exchanged securely using this method. By this means it makes sure its affirmations. Here the key is safely generated using one random prime number, a master secret key and parameter value. Intended for the secured and consistent access control limitation, an encryption which is attribute-based is used. The proposed method thus ensures the protected data transmission with exact and trustworthy validation.

In 17, the author E. Shanmugapriya enhances the privacy-preserving big data in the cloud the proposed technique makes to exhibit the innovative and efficient model.

In 18, the author Han Qiu motivates to provide both safety and privacy in the cloud-based MCPS against user behaviors such as repeated key usages through untrusted cloud servers. Fragmentation will be introduced to be combined with encryption such that the fragmented data pieces on clouds cannot be used to leak the stored data even when the key for this system is leaked. Access control model is also needed for data sharing with security and privacy, and further, especially for disease control in this MCPS network. we introduce the algorithm to selectively encrypt the data and provide a dispersion method for further storage. The basic idea is to fragment the digital data in a manner that makes different data fragments related. For instance, a small subset of the data is used to protect the rest data fragment in a lightweight manner. Then protection schemes such as encryption algorithms can be used to protect the small subset of the data with a key. A dispersion scheme is used for the storage that the encrypted small subset of the data is stored in a secure place such as the end user's personal device and the rest data fragments are stored in cloud servers for cost-saving purposes.

In 19, the author Fatemeh Rezaeibagha frames EHR system architecture for following, Secure EHR data sharing - The protection is required to provide private access to EHR. Privacy enhancement - Additional protection is provided to the private patient records by prohibiting their access by a single party. In other words, only a threshold number of authorized parties are allowed to access a private record. Policy transformation - Flexibility of handling EHR policies is possible using our policy transformation approach. Fine-grained role-based access control - Fine-grained role-based access control is provided by using ABE-based technology.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

In 20, the author Reyazur Rashid Irshad et al, proposed framework consists of three major stages, namely data collection, secured storage, and disease detection. The data are collected using IoT sensor devices. After that, the homomorphic encryption (HE) model is used for secured data storage. Finally, the disease detection framework is designed with the help of Centered Convolutional Restricted Boltzmann Machines-based whale optimization (CCRBM-WO) algorithm. The experiment is conducted on a Python-based cloud tool. The proposed system outperforms current e-healthcare solutions, according to the findings of the experiments. The accuracy, precision, F1-measure, and recall of our suggested technique are 96.87%, 97.45%, 97.78%, and 98.57%, respectively, according to the proposed method.

In 21, the authors Seyedeh Monireh Ggasemnezhad Kashikolaei provide new algorithm to allocate resources in the cloud based on the combination of ICA and firefly algorithm. The proposed method is based on a multi-population method that always tries to maintain population diversity of solutions and results in a quality response in terms of makespan, load balancing and speed of planning in an acceptable time.

In 22, the author S. Jayapradha, used the IOT devices here are Arduino Uno and sensors like heartbeat sensor, temperature sensor, eye blink sensor, ECG sensor, mems sensor and timer. Arduino Uno is a microcontroller board. This microcontroller board is based on ATmega328P. ATmega328P is a high performance microchip. It has a flash memory that has the capabilities of read-while-write. By providing powerful instructions in a single clock cycle, ATmega328P is capable of throughputs around 1MIPS per MHz (Microprocessor without Interlocked Pipeline Stages). This helps in balancing consumption of the power and speeds up the process. It has the program memory of type flash memory of 32KB. The CPU Speed is of about 20 MIPS. Arduino Uno board contains 14 digital input and output pins. Here, 6 pins can be used as Pulse Width Modulation outputs, 16 MHz quartz crystal, an ICSP (In-Circuit Serial programming) header, USB connection, reset button and a power jack. This has all the facility to support the microcontroller. Just by connecting to a computer with a USB cable is enough to start the program. This system can also be started by connecting it to an Analog or Digital circuit or by simply connecting it with a battery.

VII. PROPOSED METHODOLOGY

The proposed scheme consists of three phases, namely:1) data acquisition and sensor network phase, 2) secure cloud storage phase, 3) Data analytics and prediction process phase (fig-4 Proposed System for Secure Health Monitoring System).

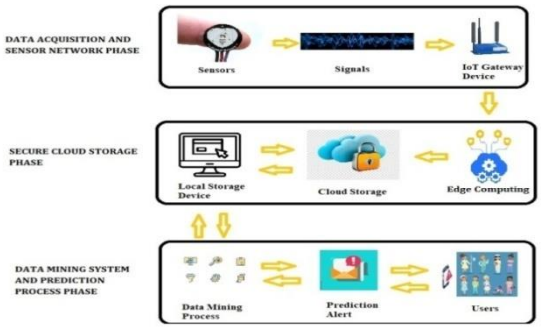

Figure 4: Proposed System for Secure Healthcare Monitoring system

In phase 1, the sensors will be transmitted the data into IOT gateway through wireless Sensor Network like ZigBee, WiFi, BlueTooth, RasPi etc. In WSN, the network needs long LifeTime for good data transmission network. So we proposed to compared Standard Firefly Algorithm and Enhanced Firefly Algorithm for Long Life Network Communication.

In phase 2, in the data acquisition phase, a person's medical records are gathered by sensors in various devices. The IOT gateway devices are then used to send the data to the edge computing. The edge server in edge computing is in charge of maintaining all the specifics of the encrypted patient data that is kept on cloud storage. Additionally, it uses clustering techniques to identify patient data that is anomalous. Every piece of information gathered by the body sensors is sent to the edge computing, which subsequently forwards it to the medical server located in the cloud storage system. In order to protect the security and integrity of patient data, this edge computing contains an encryption module with an access policy.

In phase 3, the microcontroller will be interfaced with biosensors to monitor the patient's vital signs. An SMS will be sent to the patient's caretaker and doctor if any of the sensor's pre-set threshold values are exceeded. The web server portion of the monitoring system is made up of Sensor data that will be routinely transported from the sensor network, where sensor nodes are outfitted with various biometric sensors, to the hospital database, where it will then be continuously posted to the hospital's web server. Doctors may keep an eye on the patient's status from anywhere.

In phase 1, For example, a thermometer is a sensor that can measure certain aspects of its target. Each node inside a sensor network that may collect, process, or exchange data with other nodes linked to the network is referred to as a sensor node. The necessity for each wireless sensor network to manage network lifetime maximization is one of the main challenges.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

A biosensor is a sensor that is intended to detect biological phenomena or a sensor that is integrated with a biological component; examples of biosensors include thermometers that measure blood glucose concentration and human body temperature beneath the ear. Biosensors are an analytical tool that convert biological data into an electrical signal and identify changes in biological processes. Typically, a large number of sensors are deployed at random, with the primary objective being to locate them as close to the target region as possible while yet providing adequate coverage. Deployment can be managed in certain situations, and it's crucial to guarantee maximum coverage.

On deployment, sensor nodes have to function independently with minimal resources and energy available, navigate unknown individual node locations, and use wireless communication to extend network lifetime as much as feasible. Data transfers across the whole network may cease if the critical sensor nodes at the strategic locations for the network's routing are exhausted. Any individual node inside a sensor network that may collect, process, or exchange data with other nodes linked to the network is referred to as a sensor node. The requirement for each wireless sensor network to manage network lifetime maximization is one of the main hurdles The cloud server, which is accessible from anywhere, stores the transmitted sensor data from the IOT Gateway. The physician is keeping an eye on the data (caretaker). The doctor can assess the patient's condition based on the sensors' input values. An Arduino Uno, a temperature sensor, a buzzer, a vibration sensor, an eye blink sensor, a heartbeat sensor, and a buzzer are the hardware utilized to construct this technology.

In wireless sensor networks, the sensor nodes placed at different locations detect the data and send it to the base station. A temperature sensor, an Xbee module, an Arduino board router, and multiple nodes are combined to create a wireless mesh network (WSN) using mesh technology. Xbee uses an Arduino board to sense the data and transmit it to the base station. The biosensor shown in Figure 5 is made up of three parts: the electrical circuit, the transducer, and the sensor.

Sensor or detector: The biological component that makes up the first section is the sensor or detector. It's a receptor that's biological. Through interaction with the analyte, it transmits an electrical signal indicating a change in composition.

Transducer: This physical component, which makes up the second segment, is responsible for amplifying the biochemical signal obtained from the detector, converting it into an electrical form, and presenting it in an understandable manner.

Electrical circuit: It is the component that is connected to the other parts and is made up of a display unit, a processor, and a signal conditioning unit.

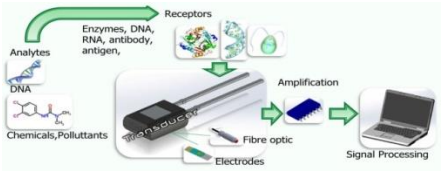

Figure –5 Components of Biosensors.

The decision-making issues within decision-making are not restricted to our everyday activities. In engineering, management, and many other fields, they are highly prevalent. Numerous academics applied the idea of optimization in a variety of fields, including as economics, computational intelligence, decision science, engineering, transportation planning, economics, agriculture, tourism, sports science, and even political science [23]. These issues are known as mathematical optimization problems when they are expressed mathematically. It will have a set of feasible activities, which are also referred to as feasible areas, and an aim, which is a performance metric for these actions. Equation (1) is a typical single objective minimization problem.

$$\boldsymbol{min_x}\{\boldsymbol{f(x)}|\boldsymbol{x} \in \boldsymbol{S} \subseteq \mathrm{R}^{\mathrm{n}}\} \qquad (1)$$

Standard Firefly Algorithm

Several metaheuristic algorithms have been introduced, many of them inspired by nature. It has used experience rather than instruction to solve problems and come up with solutions. The primary inspiration for the early metaheuristic algorithms came from natural selection and the idea of survival of the fittest [24]. Animals use a variety of communication techniques to exchange messages with one another.

Fireflies communicate by flashing. Approximately 2000 different species of fireflies exist, each with a unique flash pattern. A brief flash with a specific pattern is typically produced by them. Bioluminescence is the name of the metabolic mechanism that produces the light. Both to entice a mate and alert potential predators, they communicate by flashing. An appropriate partner will mirror the pattern of the light or respond with a different pattern based on the pattern of the light. It is also important to remember that light intensity decreases with distance, thus nearby fireflies that are within visual range of the flash will react to it when it flashes.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

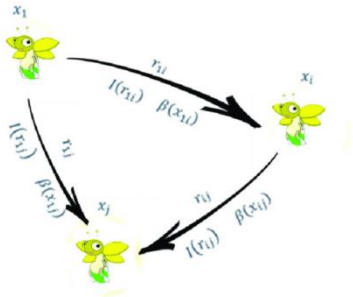

Figure 8: The Conceptual view of Firefly Algorithm

Yang (2008) introduced the FA swarm metaheuristic, which was further refined and improved. The algorithm uses the flashing lights of fireflies to simulate their interactions. Since all fireflies in Figure 8 are assumed to be unisex, any firefly can be attracted to any other firefly; a firefly's attraction is directly correlated with its brightness, which is determined by the objective function. A brighter firefly will draw the attention of other fireflies. In addition, the brightness diminishes with distance r according to the inverse square law, as expressed in Equation (2).

$$I \propto \frac{r}{2} \qquad (2)$$

If S is the feasible region, the decision variable is vector x, and the objective function is defined as f: $\mathbb{R}n \rightarrow \mathbb{R}$. If and only if $x^{-} \in S$ and $f(x^{-}) \leq f(x)$, $\forall x \in S$, then a vector, x^{-}, is said to have an optimal solution for the minimization problem stated in Eq. (1).For every x in close proximity of x′, f (x ') ≤ f (x), and x′ is a member of S. The light intensity at a distance of r from the source can be found in Eq. (3) if the light is traveling through a medium with a light absorption coefficient of γ.

$$I=I_0\, e^{-\gamma r^2} \qquad (3)$$

Where I_0 is light intensity at the source. Similarly, the brightness, β, can be given as in Eq. (4)

$$\beta = \beta_0\, e^{-\gamma r^2} \qquad (4)$$

A generalized brightness function for $\omega \geq 1$ is given in Eq. (5). In fact, any monotonically decreasing function can be used.

$$\beta = \beta_0\, e^{-\gamma r^{\omega}} \qquad (5)$$

A random feasible solution known as "fireflies" will be assigned a light intensity by the algorithm according to how well it performs in the objective function. The firefly's brightness, which is directly correlated with its light intensity, will be calculated using this intensity. In minimization issues, the highest light intensity will be awarded to the solution with the smallest functional value. Upon assigning the solutions' brightness or intensity, each firefly will trail others with higher light intensities. The firefly with the highest brightness will move randomly about its neighborhood in order to conduct a local search. Therefore, using the updating formula found in Eq. 6, firefly i will travel towards firefly j if firefly j is brighter than firefly i in a pair of fireflies.

$$x_i := x_i + \beta = \beta_0\, e^{-\gamma r_{ij}^2} (x_j - x_i) + \propto (\varepsilon() - 0.5) \qquad (6)$$

Where β_0 is the attractiveness of x_j at $r = 0$, in [5] the author recommended that $\beta_0 = 1$ for implementation, γ is an algorithm parameter which determines the degree in which the updating process depends on the distance between the two fireflies, α is an algorithm parameter for the step length of the random movement and $\varepsilon()$ is a random vector from uniform distribution with values between 0 and 1. For the brightest firefly, x_b, the second expression in Eq. (6) will be omitted, as given in Eq. (7)

$$x_b := x_b + \propto (\varepsilon() - 0.5) \qquad (7)$$

Algorithm 1: The Standard Firefly Algorithm

Set Parameter as (∝ , ɣ)

Set simulation set-up (Number of initial solutions and maximum iteration (N, MaxGen))

Randomly generate N initial solutions

for iteration = 1: n-1

Compute the brightness, I

Sort the solution in such a way that, $I_i \geq I_{i-1}$, ∀i

for I = 1:n-1

for j=i+1:n

if $I_j > I_i$

Move firefly I towards j

endif

end for

end for

move firefly N, (x_b), randomly

end for

report the best solution

The firefly locations are updated iteratively starting with algorithm 1 and continuing until a termination of the necessity is met. A maximum number of iterations, a tolerance from the known optimal value, or the absence of improvement in successive iterations can all be used as termination criteria.

Proposed to modify the movement of the brightest or dimmer firefly:

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

The initial random *N* solutions, their opposites will be generated, and the best *N* solutions will be chosen from the *N* solutions and their opposites where an opposite number for *x* is given by $x_{min} + x_{max} - x$. The brightest solution x_b will be updated as follows:

y = x_b
for *i* = 1 : *D* (for all dimensions)
for *j* = 1 : *N* (for all the solutions)
y(*i*) =x_j (*i*)
if [*f* (*y*) is better than *f* (x_b)] x_b= *y*
end if
end for
end for

Here the best solution will improve or will not change in each of the iterations.

VIII. PERFORMANCE COMPARISON METRICS

Five performance indicators are employed to evaluate the clustering performance, namely the sum of intra-cluster distances (i.e. fitness scores), average accuracy, average sensitivity, average specificity, and macro-average F-score (Fscore). The first distance-based metric is used to indicate the convergence speed of the proposed models, while the last four metrics are used as the main criteria for clustering performance comparison. We introduce each performance metric in detail, as follows.

1. Sum of intra-cluster distances: This measurement is obtained by the summation of distances between the data samples and their corresponding centroids, as defined in Eq. (8). The smaller the sum of intra-cluster distances, the more compact the partitioned clusters. Similar to KM clustering, the proposed models employ the sum of intra-cluster distances as the objective function, which is minimized during the search process.

Where C_i andZ_i, represent the ith cluster and the centroid of the ith cluster, while $O_i$and k denote the data belonging to the ith cluster, and the total number of clusters, respectively.

$$f(O,C) = \sum_{i=1}^{k} \sum_{O_i \in C_i} \sqrt{(O_i - Z_i)^2} \qquad (8)$$

2. Average accuracy: The mean clustering accuracy is obtained by averaging the accuracy rate of each class, as defined in Eq. (9). The merit of this performance metric is that it treats all classes equally, rather than being dominated by classes with a large number of samples.

$$\text{Ave\_accuracy} = \frac{\sum_{i=1}^{k} \frac{tp_i + tn_i}{tp_i + fn_i + fp_i + tn_i}}{k} \qquad (9)$$

Wheretp_i, fp_i and tn_i represent true positive, false negative, false positive and true negative of the ith cluster respectively

3. Average sensitivity: As defined in Eq. (10), sensitivity (i.e. recall) is used to measure the proportion of correctly identified positive samples over all positive samples in the data set. Similar to the average accuracy, the macro-average of sensitivity is calculated, in order to ascertain all classes are treated equally for multi-class clustering tasks.

$$\text{Ave\_sensitivity} = \frac{\sum_{i=1}^{k} \frac{tp_i}{tp_i + fn_i}}{k} \qquad (10)$$

4. Average Specificity: Specificity is used to identify the proportion of correctly identified negative samples over all negative samples in the data set [ ]. Eq. (11) is used to obtain the macro-average specificity for multiclass tasks.

$$\text{Ave\_specificity} = \frac{\sum_{i=1}^{k} \frac{tn_i}{tn_i + fp_i}}{k} \qquad (11)$$

5. Macro-average F-score ($Fscore_M$): $Fscore_M$ is a well-accepted performance metric, which is calculated based on the macro-average of precision and recall scores [ ], as defined in Eqs (12),(13),(14).

$$Fscore_M = \frac{(\sigma^2+1) * Precision_M * Recall_M}{\sigma^2 * Precision_M + Recall_M} \qquad (12)$$

$$Precision_M = \frac{\sum_{i=1}^{k} \frac{tp_i}{tp_i + fp_i}}{k} \qquad (13)$$

$$Recall_M = \frac{\sum_{i=1}^{k} \frac{tp_i}{tp_i + fn_i}}{k} \qquad (14)$$

Where σ = 1, in order to obtain equal weightings of precision and recall.

IX. EXPERIMENT ANALYSIS

In Experimental result, the research process was compared and analyzed between Firefly algorithm and enhanced Firefly algorithm based on Fitness, Accuracy, F Score, Sensitivity and Specification. From this overall analysis Enhanced Firefly Algorithm is more efficient than Firefly Algorithm.

Feature number	Criteria	FA	EFA
22	Fitness	89.649	92.611
22	Accuracy	0.7307	0.804
22	F Score	0.7063	0.7873
22	Sensitivity	0.6953	0.7467
22	Specificity	0.7660	0.8613

Table 1: Comparison between Firefly Algorithm and Enhanced Firefly Algorithm based on some criteria.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *10 September 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *30 October 2023*

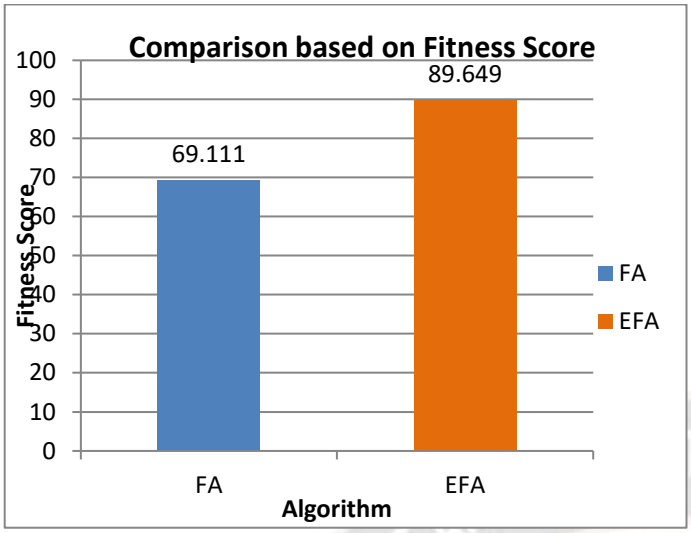

Figure 9: Comparison based on Fitness Score

In Figure 9, Comparison was done based on Fitness Score between Firefly Algorithm and Enhanced Firefly Algorithm. The Enhanced Firefly Algorithm has high fitness score of 89.649 while comparing with Firefly basics or native Firefly Algorithm is 69.111 which show that the Enhanced Firefly Algorithm has remarkable result.

In Figure 10, Comparison was done based on Fitness in overall Firefly generation between Firefly Algorithm and Enhanced Firefly Algorithm. The Enhanced Firefly Algorithm has high efficient fitness score while comparing with Firefly basics or native Firefly Algorithm which show that the Enhanced Firefly Algorithm has remarkable result.

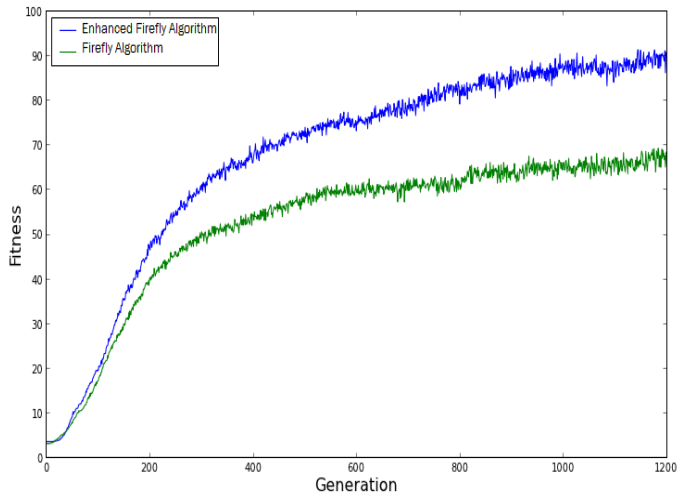

Figure: 10 Comparison based on Generation

In the Figure 11, shows performance analysis was firefly algorithm and Enhanced firefly algorithm in accuracy, probability that are combined among thus the Enhanced firefly Algorithm has high accuracy and high position value is 0.804 while comparing with Firefly Algorithm which has less accuracy value is 0.730.

In F Score, probability that are combined among thus the Enhanced firefly Algorithm has high accuracy and high position value is 0.7873 while comparing with Firefly Algorithm which has less accuracy value is 0.7063.

In Sensitivity, probability that are combined among thus the Enhanced firefly Algorithm has high accuracy and high position value is 0.7467 while comparing with Firefly Algorithm which has less accuracy value is 0.6953.

In Specificity, probability that are combined among thus the Enhanced firefly Algorithm has high accuracy and high position value is 0.8613 while comparing with Firefly Algorithm which has less accuracy value is 0.766.

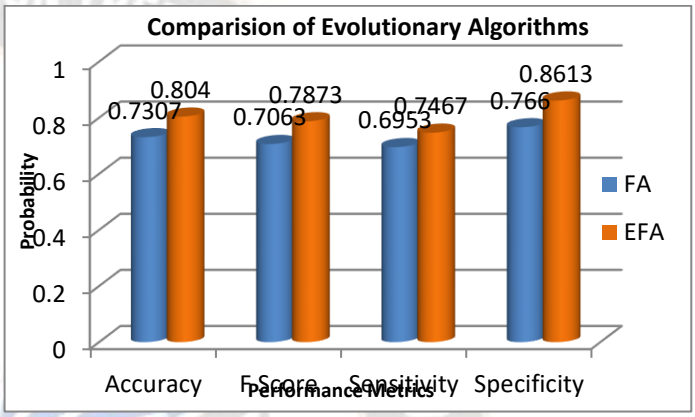

Figure: 11 Comparisons of Evolutionary Algorithms

Both an experimental result we concluded that the Enhanced firefly Algorithm is better while comparing with native Firefly Algorithm.

X. CONCLUSION AND FUTURE WORK

An enhanced approach to distributing the demands of the overloaded traditional healthcare system is through smart healthcare systems. The majority of IoT-based cloud-based smart healthcare systems are built on this foundation. However, the service latency rate of this technology is not fast enough to meet the demands of urgent, urgent healthcare needs. This research paper's primary goal is to compare the upgraded model Firefly method to the Firefly algorithm for network-long lifetime in WSNs. To implement, an enhanced Firefly algorithm and analyze a few factors, including fitness, accuracy, score, sensitivity, and a specification for an efficient method of sending sensor data to the cloud. In the future, a few of the limitations of smart healthcare will be removed by the edge layer known as edge computing which is built between IoT devices and the cloud layer.

The goal of the proposed framework is to analyze the variation of observed bio-signal values from the average or standard values in order to predict or identify the probability that an individual would have a disease. The abnormal data received from the edge device is detected by the framework. It provides

safe access to private information stored on cloud servers. To find anomalies in transmitted patient data, four distinct clustering approaches have been applied in further research process.

REFERENCES

[1] Weizhe Chen et. Al (2021),"Authorized Shared Electronic Medical Record System with Proxy Re-Encryption and Blockchain Technology", MDPI, 22 November 2021.

[2] Hesham A. El Zouka (2017),"An Authentication Scheme for Wireless Healthcare Monitoring Sensor Network", IEEE, 2017.

[3] Srinivas Jangirala et. Al, (2018), "Cloud Centric Authentication for Wearable Healthcare Monitoring System", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, 2018.

[4] Subramani Jegadeesan et. Al(2019)," Computationally efficient mutual authentication protocol for remote infant incubator monitoring system", Healthcare Technology Letters, 2019, Vol. 6, Iss. 4, pp. 92–97.

[5] Prajakta Kamble, (2019)," Digitalization of Healthcare with IoT and Cryptographic Encryption against DOS Attacks", IEEE, 2019.

[6] Waqar A. Khan et. Al(2016), "A Review and Comparative Study of Firefly Algorithm and its Modified Versions", INTECH Open Science, 2016.

[7] *Mnar Alnaghes et. Al (2016),"*An Effective Method for Secure Data Delivery in IoT",INTECH Open Science, 2016.

[8] Maria Pateraki et. Al (2019), "Biosensors and Internet of Things in smart healthcare applications: challenges and opportunities", Researchgate, 2019.

[9] Buddesab et. Al (2018),"Efficient Secure and Private Healthcare Data Transmission and Allocation in Cloud Environment", IEEE, 2018.

[10] Ashish Koirala et. Al, (2023)," Enhancing IoT Device Security through Network Attack Data Analysis Using Machine Learning Algorithms",MDPI, Published: 9 June 2023.

[11] Snehal Sanjay Kale, (2018). "A Secured IoT Based Webcare Healthcare Controlling System using BSN", (ICICCT 2018), ISBN:978-1-5386-1974-2.

[12] Ala Saleh Alluhaidan (2022). "Secure Medical Data Model Using Integrated Transformed Paillier and KLEIN Algorithm Encryption Technique with Elephant Herd Optimization for Healthcare Applications", Hindawi Journal of Healthcare Engineering, Volume 2022, Aug 22.

[13] Abdulmohsen Almalawi et.Al,(2023). "Managing Security of Healthcare Data for a Modern Healthcare System", MDPI, 30 March 2023.

[14] Kirtirajsinh Zala et. Al, (2022). "On the Design of Secured and Reliable Dynamic Access Control Scheme of Patient E-Healthcare Records in Cloud Environment", Hindawi Computational Intelligence and Neuroscience Volume 2022, 18 August 2022.

[15] Khalid K. Almuzaini et. AL,(2022), "KeyAggregation Cryptosystem and Double EncryptionMethod for Cloud-Based Intelligent Machine Learning Techniques-Based Health Monitoring Systems" Hindawi Computational Intelligence and Neuroscience Volume 2022, 21 April 2022.

[16] A. Pugazhenthi (2019), "Data Access Control and Secured Data Sharing Approach for Health Care Data in Cloud Environment" Springer, 7 June 2019.

[17] E. Shanmugapriya, (2019)," Efficient and Secure Privacy Analysis for Medical Big Data Using TDES and MKSVM with Access Control in Cloud", Springer, 5 June 2019.

[18] Han Qiu et.AL, (2019), "Secure Health Data Sharing for Medical Cyber-Physical Systems for the Healthcare 4.0", IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, VOL. , NO. , 2019.

[19] Fatemeh Rezaeibagha (2016), "Distributed clinical data sharing via dynamic access-control policytransformation", International Journal of Medical Informatics, 10 February 2016.

[20] Reyazur Rashid Irshad et. Al (2023), "An Optimization-Linked Intelligent Security Algorithm for Smart Healthcare Organizations", MDPI,15 February 2023.

[21] Seyedeh Monireh Ggasemnezhad Kashikolaei et. Al(2019),"An enhancement of task scheduling in cloud computing based on imperialist competitive algorithm and firefly algorithm", The Journal of Supercomputing, Springer 2019.

[22] S. Jayapradha, (2017), "An IOT based Human healthcare system using Arduino Uno board", International Conference on Intelligent Computing,Instrumentation and Control Technologies (ICICICT), 2017.

[23] Yong-Yuan Deng et. Al, (2017),"Internet of Things (IoT) Based Design of a Secure and Lightweight Body Area Network (BAN) Healthcare System", MDPI, 15 December 2017.

[24] Suliman Abdulmalek et. Al (), "IoT-Based Healthcare-Monitoring System towards Improving Quality of Life: A Review", MDPI, Published: 11 October 2022.

[25] Miodrag Zivkovic et. Al, (2020), "Wireless Sensor Networks Life Time Optimization Based on the Improved Firefly Algorithm",IEEE, 2020.s