Sheffield
Hallam
University

Maliciously roaming person's detection around hospital surface using intelligent cloud-edge based federated learning

GOKULAKRISHNAN, S., JARWAR, Muhammad Aslam <http://orcid.org/0000-0002-5332-1698>, ALI, Mohammed Hasan, KAMRUZZAMAN, M.M., MEENAKSHISUNDARAM, Iyapparaja, JABER, Mustafa Musa and KUMAR, R. Lakshmana

Available from Sheffield Hallam University Research Archive (SHURA) at:

https://shura.shu.ac.uk/31196/

This document is the Accepted Version [AM]

Citation:

GOKULAKRISHNAN, S., JARWAR, Muhammad Aslam, ALI, Mohammed Hasan, KAMRUZZAMAN, M.M., MEENAKSHISUNDARAM, Iyapparaja, JABER, Mustafa Musa and KUMAR, R. Lakshmana (2023). Maliciously roaming person's detection around hospital surface using intelligent cloud-edge based federated learning. Journal of Combinatorial Optimization, 45 (1): 13. [Article]

Copyright and re-use policy

See http://shura.shu.ac.uk/information.html

Sheffield Hallam University Research Archive
http://shura.shu.ac.uk

Maliciously roaming person's detection aroundhospital surface using intelligent cloud-edge based federated learning

S. Gokulakrishnan, Muhammad Aslam Jarwar, Mohammed Hasan Ali, M. M. Kamruzzaman, Iyapparaja Meenakshisundaram, Mustafa Musa Jaber, R. Lakshmana Kumar

Abstract

As an innovative strategy, cloud-edge-based federated learning has been considered a suitable option in supporting applications in the internet of things that detect the roaming person features around the hospital surface. By connecting the internet with physical objects and transmitting information to detect the issue of maliciously roaming person features, the Internet of Things with the cloud-edge based federated learning enables the integration of the natural world and the data world, thus making life more innovative and more secure. In this study, intelligent and efficient maliciously roaming person features detection around hospital surface using cloud-edge based federated learning is proposed with the technique of internet of things of Hilbert Spectrum and cognitive dimensionality reduction with the drone tool and sensor-enabled camera. Hilbert spectrum is a statistical tool used to distinguish among a mixture of moving signals. Cognitive dimensionality reduction is a category of unsupervised machine learning techniques that helps reduce the number of features in a dataset. The proposed result was compared to existing approaches. Based on the investigation of the expertimental analysis, the Classification Accuracy of normal human findings is 18.61%, and suspicious human finding is 48.41%. Standard and patient findings are 69.95% higher than the moving data object count and response time. Classification accuracy of both standard and patient findings is 69.95% higher than the moving data object count and response time. The moving data object count is calculated concerning the response time 3.89 times higher, Precision 0.39 times higher, and recall 68% higher than the existing system.

Keywords Federated learning · Healthcare · IoT · Grid computing · Cognitive dimensionality · Hilbert spectrum · Hospital surface

Abbreviations

IoT	Internet of Things
SAGIN	Space-air-ground integrated environment
WLAN	Wireless local area network
MIMO	Multi input multi output
IT	Information technology
RAN	Radio access network
RFID	Radio frequency identification
IIOT	Industrial Internet of Things
FWA	Fixed wireless access
GPS	Global positioning system
ML	Machine learning
DL	Deep learning
SVM	Support vector machine
UAV	Unnamed aerial vehicle
FFT	Fast Fourier transform
TTF	Tensor flow federation
AI	Artificial intelligence
TP	True Positive
FP	False positive

1 Introduction

The cloud–edge-based federated learning architecture offers unique features and enhanced quality of service. There are still many challenges to the security concerns in the detection features. The research on edge network security is still in the development stage. This study focuses on the intelligent and efficient maliciously roaming person features detection around hospital surfaces using cloud-edge-based federated learning in the internet of things and Hilbert spectrum and cognitive dimensionality reduction under the grid computing platform. Data analysis is the methodical application of intellectual and/or empirical methods to explain and demonstrate, summarize and assess, and analyses information. Businesses may build goods, analyse their advertising efforts, customise material, as well as establish digital strategy with the use of data analysis. It can eventually help firms enhance efficiency and raise their bottom margin. The data analysis in the proposed system is used to build the actual participants and tools and detect the suspicious person in the hospital from the received signal from the camera and sensor. The functional description of devices was based on the IoT-enabled drone explanation, IoT-enabled camera with sensor, the controller of the IoT-enabled drone explanation, and the camera with the sensor (Kishor et al. 2021). Robust methods begin with any basic layout estimates and provide some rather a certainty (referred to as being universally converging to a localized lowest value). When opposed to methods without a confirmation of completion, durable methods normally need to do a few more computations throughout every repetition. The robust position estimation algorithm establishes the suspicious person's position estimation. In this study, the targeted projection pursuit is implemented for three purposes. The cloud-edge-based federated learning for data analysis, Information visualization for suspicious person position, and feature selection based on the adverse person reaction (sensor signal-based activities). For Cognitive result intimation to recollect inspector, the analysis of n-way arrays and non-linear dimensionality reduction, the process of getting the data from the sensor, and the process of sending the data intimation to recollect inspector is established. The working principle for IoT-enabled drones and IoT-enabled cameras with sensors is obtained (Alimi et al. 2021). The result closes with analyzing the internet of things for healthcare and efficient maliciously roaming person features detection around hospital surfaces using cloud-edge-based federated learning. The principal contributions of this paper are:

- This study focuses on the Intelligent and efficient maliciously roaming person features detection around hospital surfaces using Cloud-Edge-based Federated Learning.
- The robust position estimation algorithm establishes the suspicious person's position estimation.
- The working principle for IoT-enabled drones and the working principle of IoT-enabled cameras with sensors is achieved. The targeted projection pursuit is obtained by cloud edge-based federated learning and Information visualization.
- The functional description of devices was based on the IoT enabled Drone explanation and IoT-enabled camera with the sensor.

The paper is structured as follows. Section 2 provides the required background and related work, Sect. 3 details the architecture of the Proposed methodology, such as the Cloud-edge based computing, IoT-enabled features, the Hilbert spectrum, Cognitive Dimensionality Reduction, and Sect. 4 discusses the analysis and experiments of the proposed methodology, Sect. 5 concludes the conclusion with the future directions.

2 Literature review

The 6G networks for mobile have a space air-ground integrated network in the environment; this novel technology makes the healthcare information of the physical connection and the vulnerabilities of the radio and the MIMI technology. The architecture of the SAGIN, or space-air-ground central system, remains in its infancy. The WiMAX, wireless local area network (WLAN), 2G, 3G, 4G, 5G, as well as perhaps 6G technologies are used by the grounding telecommunication (GCom) infrastructure. This MIMO and the artificial intelligence technology act as the data protection and privacy technique to secure the health-related data in the promising methods. This data protection is recognized as the platform of the agnostic security of differential privacy. In the area of information technologies (IT), the term agnostic alludes to anything that has been generalized to allow for network interoperability. The phrase may be used to describe both corporate procedures or operations in addition to technology as well as equipment. Here the excellent technique will be used to distribute the magnitude of the attack to substantiate the data breaches (Nguyen et al. 2021). Various data channels should be delivered or collected among exactly one machine at a moment in order for Single User MIMO to function. For this innovation to work, MIMO technique as well as numerous antennae must be supported by both the sending and reception Wi-Fi devices. Whereas the 802.11ac standard's second wave was the first to include MU-MIMO.

The services and the multimedia application for the various interconnection contain the solution of the multimedia services. This service act as fixed wireless access. This wireless access creates many challenges in the network; these challenges are considered the subsequent increase of the network requirements. Here in this paper, the broadband schemas, the transport options for the RAN, and the technical fact that act as the transport of the 5G network are confirmed. The solution of the vehicle of the RAN functions is formed. Accessibility to and administration of assets between broadcast stations are facilitated by a RAN. The RAN transmits its signals to multiple wireless terminals so it may transit with data from other networking, as well as a telephone or even other equipment is securely attached to the backhaul, or base stations. This paper suggested the dynamic nature of the FWA network solution (Alimi et al. 2021).

The IIOT is randomly increasingly in the significance of the evolution of the RFID to find the radio frequency for the wireless network for the autonomous vehicles and the intelligence of the things in the formation of the paradigm for the trustworthy in the industrial for the application of the business and the domains of the industries this industry maintains the collaboration of the communication and the Self-maintenance, self-healing, and the operation behavior for the implementation of the accomplish of the uncertainties of the real-time interaction for the efficiency of the humans and the exchange of the computer. The IoT application involves robotic interactions. The robot and the humans will make equal interactions among the technologies in the taxonomies for the literature.

Edge computing is used in the mobile storage in the end-user for the data sources. This data source reconnects the cloud computing for the leveraged for the heterogeneous in the argument reality of the runtime optimization. This runtime optimization has the drawbacks of the common application of the problems in the industry solution for the research challenges for the expected computing for the surface of the components, this component and the classification of the features in the data store will be stored this storing of the data will be done in the composition of the applications.

In healthcare, the global fog architecture is compared with the competency of the various fog applications. The interface, gateway, as well as corporate levels make up the three-tier architectural paradigm. In handling the transmission of data as well as management streams engaged in user behavior, different levels have unique responsibilities to perform. Three connections link them together. Utilizing the vicinity networks, the edges tier gathers information from the different nodes. This fog application makes the centralized and the decentralized of the cloud and the fog computing for the storage and the model of the three-tire application in the IoT scenario; this scenario will make the computing architecture for the period in the fog computing. A 3-tier design has advantages in terms of better transversal expansion, efficiency, as well as reliability. When there are three layers, every component can be produced simultaneously by a separate group of programmers using a separate programming technology than the producers of the other levels. This fog computing architecture and the combination of the IoT scenario for the fog computing for the innovation in the pertaining of the IoT sensors for the IoT.

3 Roaming person data analysis using data from sensors

The hospital environment data is collected by the drone and used to visualize 2D and 3D, recorded by the site. Data visualization aids in the method of translating and graphically presenting health information elements that streamline and synthesize the study of difficult-to-process, massive data. This includes the slope models for measuring the length, volume, and stockpile. This is a tool that is used primarily for the Arial data. This raw material construction makes the traditional process in the inventory analysis. By using inventory analysis, one can decide how much goods to maintain on available to increase supply without going overboard with storage costs. Inventory is a financial statement item that reflects the goods a business ultimately intends to sell to consumers. Many companies, hospitals, and property or an instrument use drone analytics to quickly inspect the roof images and the insights. A drone is basically a hovering robotic that can be augmented with wireless or flown on its own utilizing scheduled flights that are managed by computer as well as internal instruments or a global positioning system (GPS). Drones and artificial intelligence will make the data processing. This data processing was found to make the company deal with drone management. Generally, the sophisticated characteristics make human intelligence for solving the problem for the machine and the deep learning in the artificial intelligence process.

Tracking is a challenging process with computer vision devices like detecting the motion of a person, analyzing the object and recognizing things and surveillance, and so on. The illumination, lenses, imaging system, visual processor, and connectivity are the main parts of a human imaging technology. Computer vision techniques find physical features in photos and contrast them with human profiling datasets. Facial recognition technology is used by smart phones to verify the identity of its users. Social networking applications identify and tag individuals using face detection. The tracking process is considered difficult due to the complexity of backgrounds and the changes in the scale due to the movements of the objects. Accurate object tracking is only obtained through the online tracking system by updating the trajectories in the frame of the particular things. The goal of the tracking system is to track the objects moving with the image sequences.

Pseudocode for information visualization for a suspicious person's position

```
Input; initially, the rectangle frame surrounding the object $R_o$
Initialize; $c \leftarrow 0$
For $k=1,2\ldots n$
    $c \leftarrow c+1$
    Extract ← frame $R_k$
    $R_k \leftarrow R_{k-1}$
    Compute $D_v \leftarrow (R_{k-1} - R_k)$
    Apply $R_o \leftarrow D_v$
    Extract $\leftarrow R_k$
    If $(c=10)$
        $\Theta=(V(k+k+j)-(V(k+j,\ k+j+10)))$
        $c \leftarrow 0$
    End if
    If $|\Theta| > \pi/2$
        Suspicious person position detection
        Tracking the object
    End if
End for
```

Object tracking is an essential part of the representation of targets; thus, the features of objects like contours, edges, and descriptors with global statistics were used for the object tracking process (Gedeon et al. 2019). The input for the object tracking system is the rectangle frame surrounding the object $R_o$at the beginning of the process. The different structures need to be used to determine the various things in the dataset, and it is represented as follows,

$$S(T + 1) = |A(m, n, T + 1) - A(m, n, T) \tag{1}$$

where T is the time frame assumed based on the surroundings of the object, as the various images only have some pixels with the intensity values, which will be varied between the frames. The object tracking accuracy is wholly based on the speed of the moving image, i.e., the faster the movements need a higher number of thresholds. The background of the image, where the image contains only the experience with the pictures are, averaged based on the series. Thus the knowledge of the image can be calculated as follows,

$$D(m, n) = \frac{1}{L} {}_{j=1}^{L} A(m, n, T \quad 1) \tag{2}$$

where T is the number of time series, and N is the number of images taken from the average value; thus, it represents the pixel of the particular embodiment that is taken as the input. It will also be based on the number of images moved per second (Sharma et al. 2021). Hence, the threshold value can be generated after calculating the image background.

3.1 Computer vision for monitoring the patient in a hospital

To monitor the deep patient learning and the specialized machine learning method for the interconnection of the neurons in the technical learning method. The Graphic processing unit and the deep understanding make the infrastructure for the images captured by the drone camera. Here the image recognition and the feature extraction process are done for the image recognition of the DL and ML metamethods. The data collection is done and sent to the image recognition using the wireless network using the IoT sensors. If the technique or structure of packet forwarding is unimportant to the operation of the device or application, it is referred to as agnostic or data agnostic in technology. This indicates that the system or application can access information successfully even when it is delivered in various forms or comes from various origins. The malicious roaming person can be detected in this vision, and its feature extraction is done.

Malicious activities are observed with the help of the drone. In the Fig. 1 mentioned earlier. 1, drone roaming is used to capture information about the hospital for safety purposes. Thus, the drone is used to collect all the data regarding the hospital environment. Then it transmits the data to edge computing. This edge computing also receives the information from the communication network. The communication network is considered to take complete control of the base station and act as the security in charge (Gedeon et al. 2019). This security in the account will classify the images with the help of a deep learning algorithm.

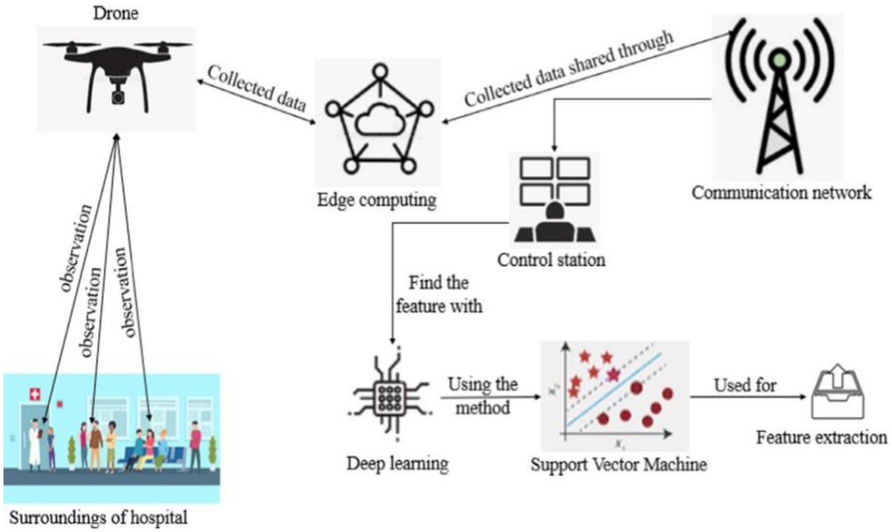
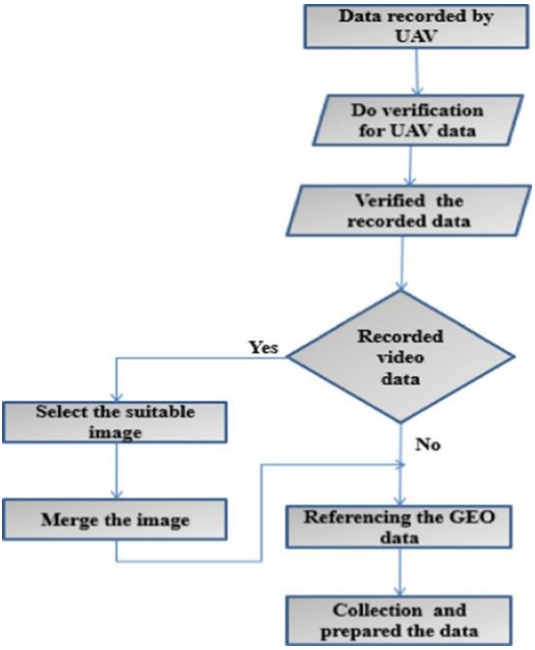


Fig. 1 Intelligent maliciously roaming person detection around hospital surface using drone

The deep learning algorithm is mainly used for the classification process. The support vector machine in deep learning helps manage the system's elements for the feature extraction process. Then these extracted features will make the SVM for the support vector in forming the components; this feature extraction will enable the hospitality data, and then the IoT is enabled with the drone system. This drone system has to allow for collecting the data in the form of a video signal. Even though drones are robust devices, extremes in heat, moisture, or weather might have an impact on the drone's connectivity as well as flying steadiness. This is due to the fact that the drone's distance is reduced by these harsh weather circumstances or radio transmission strength. Methods are used by machine learning to interpret information, understand from those statistics, as well as generate wise judgments depending on what it has discovered. Deep learning organises algorithms into levels to produce an artificial neural system that is capable of independent training as well as deductive reasoning. A part of machine learning is called computational modelling. This gathered information is processed with a deep learning algorithm to find the malicious activity in the hospital's surroundings. This deep learning has to make the classification of the drone capture images (Naeem et al. 2019). Hence, a systematic function or view is required to find the captured data in the image or video format to view the data collected from the drone.

The above Fig. 1 represents the overall process of data analysis. The analysis begins with the data collection in this system. The data will be collected only through UAVs or Drones. It is the device used to manage real-time data, mainly for monitoring, surveillance, etc. The data collected from the drones will be stored in the internal memory or desktop or the server based on the importance of the data. The information gathering with the drone and analysis contains specific steps: data collection, verifying the data; data classification; calculation of indices, and finally, obtaining the results.

Fig. 2 Process for data analysis


Data recorded by UAV
Do verification for UAV data
Verified the recorded data
Recorded video data
Yes
No
Select the suitable image
Merge the image
Referencing the GEO data
Collection and prepared the data

From Fig. 2, data collection is the process of gathering information from the UAV devices, which are often used in collecting the high and long way of the data collection process. The compiled data need to check for a suitable image and GEO data. All relevant photos will be merged for analysis. The collected data need to be pre-processed before analyzing. It is done by applying specific filters to obtain good quality data by gathering the loose data and then reducing the noise contained in the data while extracting it from the network. After the pre-processing method, the processed data are removed. The modelling training process will take longer as well as the quantity of data will rise if this duplicate information is left in. Additionally, because additional recordings impede the evaluation and emphasize repeating variables, the system may not produce correct findings. The features are classified with the SVM machine learning algorithm to improve the tracking process effectively (Naeem et al. 2019). Finally, the data collection after analysis will be obtained for the action tracking or recognition of a person for finding the person's malicious activity. This feature enables the system to produce the system's formation to manage the system's information to make the pixels for the system to create the intervention of the system to make the drone system enabled by the feature extraction.

3.2 Suspicious person reaction based on feature selection method using sensor signal

The suspicious person's reaction is monitored. The video data collection is done for the feature selection and the cross-correlation to detect the sensor data. The data received from the sensor is collected, and the cross-correlation instruction detection system is done for the video and the image data. This data will be compared with the cuttlefish algorithm for the experiment for the different classifiers. The network and the intelligence for the other security devices make the common compromise of the computer system; this system enables the administration of the outline detection of the other system known as the IDs. This can recognize the attackers through the feature selections.

3.2.1 Feature selection

The feature selection is the method used to reduce the total number of variables considered for input while constructing the predictive model. The main advantage of the selecting feature is that it reduces the input variables and the cost required for the computational process and improves the model performance (Nguyen et al. 2021). The machine learning algorithms are used to obtain the model's features: logistic regression, naïve Bayes, and support vector machine (SVM). Still, in this article, we use SVM to detect the malicious movement of the patients or caretakers in the hospital. The SVM is the supervised machine learning method used for the classification process. It is generally used in the statistical learning model for training classifiers. SVM categorises information items even if they are not generally differentiable by translating the information to a high-dimensional training dataset. Once a divider among the classifications is identified, the information is converted to enable the support vectors representation of the separation. The SVM contains the features determined as the classification of features, which is helpful for the decision-making process. The unique part of the SVM is as follows, effective in high dimensional feature extraction and decision making based on the original set of data used for training with the support vectors. It is also used for non-linear data. The algorithm for feature selection with SVM is as follows,

3.2.2 Variables

Classifier (4) ={SVM, NB, ID3, logistic}.

feature selection (10) = {chi-R, GR-R, IG-R, CSE-RS, CSE-GSS, CSE-BFS, CFS-RS, CFS-GSS, CFS-BFS, WFS}.

Pseudocode for feature selection based on the suspicious person detection

```
Input;classifier (4), feature selection fs (10)
For (j ε 1, 2s...4)
    For (k=1ε 1, 2...10)
        Apply fs (k)
        Classify← Classifier (j)
        For (i= 1, 2…n)
        |   If ($X_{j,k} \approx X_k$)
                N←N+1
        End for
        A (j) (i) =$\frac{N}{n*100}$
        The result, A (j) (i)
    End for
End for
```

In choosing the feature space from the original data with the selected subset for the feature selection, thus the total number of features in the data will increase the time taken for computation, affecting the classifier based on the accuracy (Smys and Raj 2019). The subsets feasible for selecting the features are considered only by evaluating the datasets. The feature is regarded as "Ft," defined based on the vectors determined as L and J. It is considered to be the feature space of the raw data.

$$Ft = \{L_1, L_2, \ldots L_n, J_1, J_2, \ldots J_n\} \tag{3}$$

where L is the number of vectors of n datasets, and J is the indicator for the vectors where some indicators are more suspicious. The variables for feature selection were as follows, feature selection (10)={chi-R, GR-R, IG-R, CSE-RS, CSE-GSS, CSE-BFS, CFS-RS, CFS-GSS, CFS-BFS, WFS}, here hence the 10 number of variables were considered for feature selection process (Qayyum et al. 2021). Thus, the SVM extracts the feature only through the high dimensional mapping of features; thus, the vectors or data points can be easily classified also when the features are not separated linearly; hence the SVM is as follows,

$$G(M) = W^T M + C \tag{4}$$

where T is the time–frequency, C is the constant, and W is the weight of the dataset. The data set will be separated linearly with the mapped features to the higher dimensional plane. If a linear relation can be used to distinguish between positive and negative items in a two-dimensional information, we declare that the data source is differentiable. The following is the equation used for obtaining the feature maps,

$$G(M, N) = \sum_{j=1}^{\infty} \lambda_j \emptyset_j(M).\emptyset_j \forall \lambda_j > 0 \tag{5}$$

The SVM algorithm with the feature extraction, classification, and mapping process effectively detects malicious movements of the persons in the hospitals. There are two main methods for analysing ransomware: dynamic analysis, that involves running the virus on the machine as well as watching it in action, and debugging. Studying the data traffic that the virus uses is one method of identifying it. This performance of the network can be used to spot malicious programs utilizing computer vision.

3.3 Drone controller with the camera using IoT sensor

Here the drone will be controlled using smart devices with the help of smartphones and the game controller. The drone controller is called the drone transmitter as well. The drone flight controller works for the signal to identify the audio and the video to find the person roaming in the hospital environment with a malicious mind. Using GPS, the drone is made to record the audio and the video signal for the feature and the audio extractions:

Figure 3 states that the drone collects the video data by roaming in someplace to collect data. The video data is processed to extract the frames, i.e., to collect data in the image format by splitting based on the structures. Then this is applied to the video

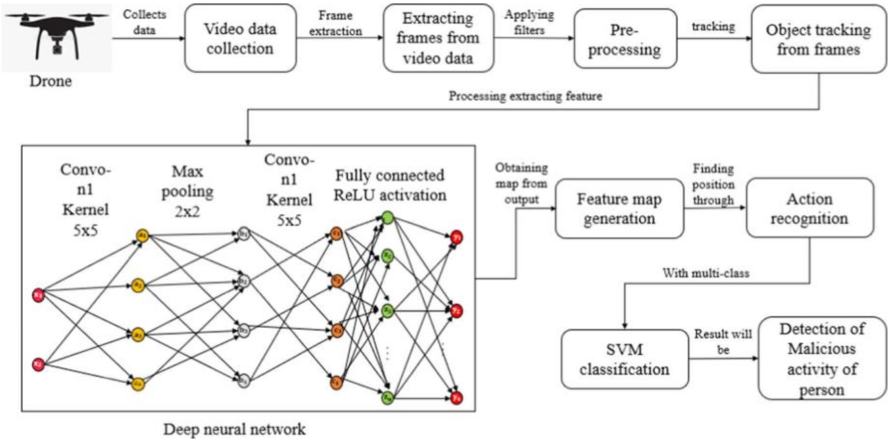


Fig. 3 Process of detecting the malicious roaming person through feature extraction

frame by processing. The pre-processing of the edges is based on the filters to remove unwanted data from the framed data, and it also increases the quality of data (Suresh et al. 2019). This tracking of the frames helps to make the image feature extraction. This feature extraction is helpful in the detection of the malicious activity of the person in or around the hospital is tracked by forming the extraction of the images and the kernel of the deep learning neural network; this neural network helps to make the formation of the system produce the innovations of the system to produce the drone for the roaming person.

This deep learning neural network is utilized to generate the output of the feature generation. The feature extraction takes place for the allocation of the frames. The videos this video recognizes the action, and this action will form the data into the support vector machine, which takes effort towards the malicious data this data by the classification of the extraction process for the support vector machine, which is classified in the form of the video images these images form the feature map generation of the system to function in the drone system this drone system helps in the formation of the system in the extraction of the videos. Deep learning is used to find the action and movement of a person with the help of data collected from the sensor. The signals generated by the sensor are processed for feature extraction to track the malicious activity of a person.

3.4 Hilbert and Fourier spectrum process for image processing:

These transforms play a very significant role in the analytical function for the contributions of the signal processing for the consideration of the electrical nature and the concepts for the Hilbert transforms for the video transmission for adopting of the offline image in the application of the image and the video transmissions (Ahmad et al. 2019). A quantitative approach called the Hilbert spectrum can aid in sorting through a jumble of transmitting information. Through the use of autonomous analysis method, the signal is split into its relevant source elements. An essential technique for image recognition, the Fourier Transform breaks down a visual into its sine as well as cosine elements. Whereas the source picture is the comparable in the feature space, the outcome of the conversion depicts the photograph in the Fourier or spectral analysis. The drone data that is the image and the video is then sent to the Hilbert and the Fourier spectrum; thus, the system's formation makes the extraction and find the construction of the system to produce the innovations of the wide and the image pre-processing. Here the conversion of the FFT is done in the linear delay of the component phase.

In Fig. 4, the data from the sensor is collected by the drones then pre-processing of the sliding window for the object detection task is used to train the classifier. The classifier is utilized to monitor the object. This process has two transformations, namely Hilbert and the Fourier transformation. This transforms the data from the waveform, which exactly forms the innovations of the Fourier and the Hilbert spectrum. In this, the sensor's frequency makes the system produce the invention of the system, in the formation of the range in the deep neural network of the time-based frequency modulation of the design for the time–frequency this frequency for modulation to be acted as a deep neural network. This deep neural network has the formation of the

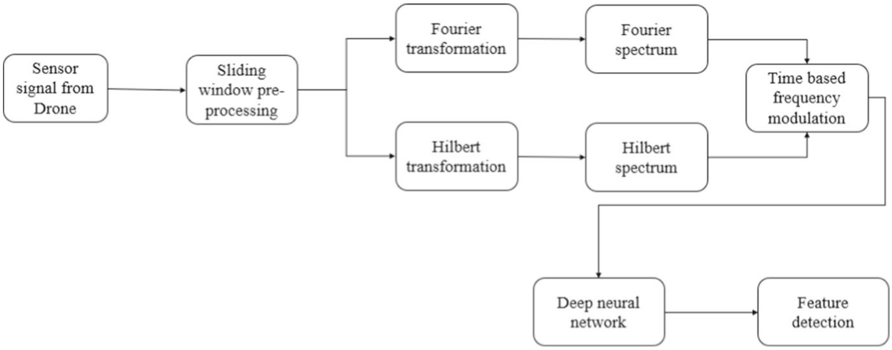


Fig. 4 Hilbert and Fourier spectrum process for image processing

feature in the detection of the feature in the construction of the system in the image of the frequency in the design of the spectrum in the formation of the improvement of the system. The innovation in the deep neural network for the transformation is in progress for the modification's feature selection.

The neural network makes the functions of the Fourier spectrum for the image processing this image processing for the transformation of the system in the digitized value of the detection of the feature. These two transformations are used in the digital transformation and the detection of the images.

3.5 Drone and camera analysis using federated learning

Network computing has the cantered computing for the new revolution of automatic image recognition in drones. This drone recognizes the data gathering and the privacy of the data for preserving the federated mixing for the significant difference in the different memory (Vermesan et al. 2020). The frequency of the images and the audio maintain the statistical heterogeneity for the aggregation problem for the naïve contribution of the data privacy of the revolutionary network for the UAV recognition of the images. They created the open-source TensorFlow Federation (TFF) Python 3 technology for federated learning. Its requirement to incorporate portable typing suggestions as well as on searching was the primary driving force underlying TFF.

3.5.1 Edge detection for the malicious activity

The edge-based detection of the data, the image, and the video analysis are done for the router's communication to the network-based detection of the malicious activity. Instead of transmitting IoT information upstream to a mainframe or cloud, edge computing, a technique for processing on site wherever information is received or utilized, enables IoT information to be captured and handled at the edges. IoT and cloud technologies work seamlessly to quickly evaluate information in real time. This malicious activity categorizes the hidden services for the edge computing for the terminal devices for the network using the communication technology. The transfer of the good standard content of the computing system produces the loading of the video data in the hospital environment. This is analyzed by the IoT network with sensor-based applications (Wu et al. 2020a). Edge computing's goal is to move the programs nearer to the locations wherever information is generated and wherever action is required. One can accomplish substantially quicker mental capabilities by doing this (Almost no time passes between an incident and a reaction). By forcing cloud computing to use the identical networking as well as risk mitigation concepts to represent position and vehicle movement, edge computing alters the safety landscape. Edge computing might demand accessibility permissions for consumers more than a substantially greater variety of endpoints, therefore IT organizations will have to explicitly plan out access permissions.

In Fig. 5, Federal learning is the algorithm with the cross decentralized devices for the local data. This federal learning typical structure of the centralized server for the factors that affect the system for invading the local data. Hence, it acts as the aggregation of the cloud (Qayyum et al. 2021).

The aggregation is used for training and testing as input from the cloud aggregation. Specifically stated, cloud integrators are eminent experts or builders who bundle several cloud storages and provide them to clients as a single, cohesive offering. A business's other option is to try to do this internally, which often leads to an untenable variety of cloud implementations around the firm. This aggregation contains the

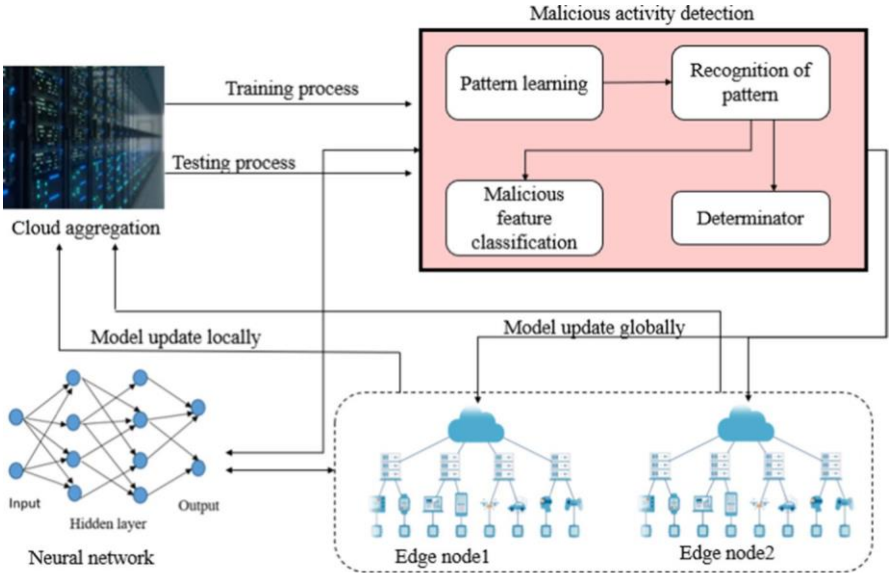


Fig. 5 Federated Learning based on Cloud-Edge

system's formation for the innovations of malicious activity detection. In order to stop hackers from accessing networking, ID/IP systems identify harmful behavior in channels as well as notify the customer. They are often recognized using well-known characteristics and typical assault types. In the event of hazards including security breaches, this is helpful. This activity enables the construction of the system to produce the patient learning for the pattern recognition of the system generates the accumulator and the determinate vary the progressive of the model update locally this updating of the local and the up-gradation of the local innovations takes place in the formation of the studies for the edge model this edge model (Wu et al. 2020b). Thus, the explanation of the diagrams is in the edge node. This edge node contains some factors that affect the system's progress to protection in nature, and the node act as the saving of the cloud system with the help of the edge. This edge produces the formation of the studies in the system's innovation to form the factors that make the formation of the cloud-based edge. This edge formulates the invention in the hidden layer (Raad 2020).

3.5.2 Algorithm for cloud-edge-based federated learning

Federated learning is the decentralized dataset that helps train the model. Federated learning provides a mechanism to unleash resources to fuel novel AI applications by training AI algorithms without letting anybody view or access the knowledge. Federated learning may take advantage of the compute capability of network edge as well as the information gathered on highly fragmented endpoints, making it a good fit for edge computer systems. We must overcome a variety of technological obstacles in order to create that kind of an edge federated teaching method. The data from the clients are considered local, and the server updates help obtain a certain level of performance by the updated parameters; it also helps in the effective data collection and reduces the cost of processing. Then, edge computing is based on federated learning with deep learning techniques, which helps train the system collaboratively based on network optimization. The federated learning method with the cloud edge network consists of the following advant: ages it will reduce the size and amount of data for communication; it also increases the involvement of network bandwidth; it helps in the real-time decision-making process will help to ensure the privacy of edge devices. The steps involved in the federated learning based on the cloud edge are initializing tasks, local model training, and global model aggregation.

Server executes

```
Initialize; r₀
For each round, T=1…2
    b→ max(K.C,1)
    S_c← set of n clients
    For each c ε S_c
        Update $r^{c}_{T+1}$←(c, r_T)
        Update $r_{T+1} = \sum_{c=1}^{C} \frac{n_c}{n} r^{c}_{T+1}$
        Update (c, r_T)
        α← split into batches
        For each epoch j ε 1to N
            For M ε α
                r← r -μΔL(r;m)
            End for
        The end for End for End for
Return r to server
```

The learning process begins with the initialization with the specific interval with the particular number of devices, after specifying the training task based on the data requirements and the target application. The hyperparameters related to the process of training and models of the server set the learning rate. Mainly it initializes the weights by initializing the consequences of the server after determining the devices with the selected parameters (Suresh et al. 2019). The receiver receives the global model W^{T}_{Gm} here t states the interaction index, then the entire updates the participants of local parameter model based on the device is communicated as W^{T}_{j} where j is the objective of clients and t is the time iteration, then the loss function is stated as

$$\mathrm{Lf}\ \dot{W}^{T}_{j}\ \Sigma \qquad (6)$$

Lf is the loss function, j is the objective, and T is the time iteration.

The local model parameter is updated and transmitted to the parameters of federated learning, and it is determined as follows,

$$W_j^T = \arg\min \mathrm{L}\, f \;\dot{}\; W_j^T \;\Sigma \tag{7}$$

This model helps update the learning process parameters to the server. The server gets the local parameters with the help of each global aggregation and the other participants in the local model. It then transmits the updated parameters of the international model. It is stated as

$$+W_{Gm}^{T\;1} \tag{8}$$

This helps to reduce the loss function of the global model $Lf \;\dot{}\; W_{Gm}^{T} \;\Sigma$ By transmitting back to the clients in the network. Hence, repeating the local and global model aggregation until the global model achieves the optimal accuracy level. Hidden layer act as the node detection method. There is no visible connectivity between the Hidden networks and the external reality (hence the name hidden). They carry out calculations and transmit data between the source as well as destination networks. A Hidden Layer is made up of a number of input layers. This method generates the factors which affect the innovation of the malicious activity of the segmentation of the images and the classification of the image in the formulation of the things to form the factors that make the locality and the mobility of a system (Kumar et al. 2019).

4 Result analysis

The Internet of Things refers to a system of interrelated, internet-connected objects that can collect and transfer data over a wireless network without human intervention. The Hilbert spectrum obtains the minimum-phase response from a spectral analysis. Dimensionality reduction reduces the number of variables in high-dimensional data while keeping as much variability in the original data as possible. Grid computing is leveraging multiple computers, often geographically distributed but connected by networks, to work together to accomplish joint tasks. Grid computing is used to analyze real-time data to find a particular pattern. Experiment with modeling to create new designs. They are verifying existing models for accuracy using simulation activities. The proposed system is used to Analysis of Internet of Things for Healthcare and efficient maliciously roaming person features detection around hospital surfaces using Cloud-Edge-based Federated Learning (Kishor et al. 2021). This approximate result is 76.8% efficient.

$$\mathrm{x} = \frac{t}{n * 100} \tag{9}$$

classification accuracy is equal to t divided by n multiplied hundred. t represents correct classification, and n represents several samples. Table 1 shows the Classification Accuracy of normal human findings vs. Moving data object count and Response Time.

Table 1 Classification Accuracy normal human finding versus Moving data object count and Response Time

No. of samples (n)	Correct classification (t)	Classification accuracy (x) (%)	Response time (ms)	Data count
20	18.17	93.0500	10	10
30	17.73	60.5667	10.5	15
40	17.29	44.3250	20	20
50	16.85	34.5800	20.5	25
60	16.41	28.0833	30	30
70	15.97	23.4429	30.5	35
80	15.53	19.9625	40	40
90	15.09	17.2556	40.5	45
100	14.65	15.0900	50	50
110	14.21	13.3182	50.5	55
120	13.77	11.8417	60	60
130	13.33	10.5923	60.5	65
140	12.89	9.5214	70	70
150	18.61	8.5933	70.5	75

The classification accuracy is the ratio of correct predictions to the total number of input samples.

The Above Fig. 6. Classification Accuracy normal human finding is based on several samples and classification accuracy. This graph comparison result compares the proposed cloud-edge-based federated learning system and the existing personalized federated education system. The proposed method of cloud-edge-based federated learning is 32% efficient.

$$\text{Response time } = \frac{n}{r} - t \tag{10}$$

Table 2 shows object Counting counts the number of object instances in a single image or video sequence (Raad 2020). Response time is equal to n divided by r and minus t. n represents data count, r represents data rate, and t represents time. Classification Accuracy suspicious human finding vs. Moving data object count and Response Time is based on moving data object count and classification accuracy.

Above Fig. 7, The Classification Accuracy is questionable human finding comparison result is a proposed system of cloud-edge-based federated learning and an existing human activity recognition system (Qayyum et al. 2021). The proposed method of cloud-edge-based federated learning is 53.6% efficient.

$$\text{Response time } = \frac{n}{r} - t \tag{11}$$

Table 3 shows The Classification Accuracy both normal and patient finding vs.

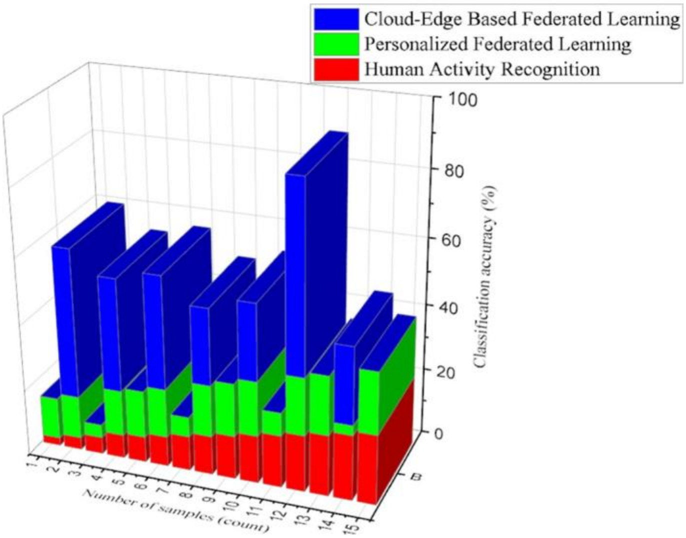


Fig. 6 Classification accuracy normal human finding

Table 2 Classification accuracy suspicious human finding versus Moving data object count and response time

Data count (n)	Data rate (R)	Time (t) (Sec)	Response time (ms)	Classification accuracy (%)
10	0.67	0.5	14.425	50.000
15	0.9	1	15.667	66.667
20	1.13	1.5	16.199	75.000
25	1.36	2	16.382	80.000
30	1.59	2.5	16.368	83.333
35	1.82	3	16.231	85.714
40	2.05	3.5	16.012	87.500
45	2.28	4	15.737	88.889
50	2.51	4.5	15.420	90.000
55	2.74	5	15.073	90.909
60	2.97	5.5	14.702	91.667
65	3.2	6	14.313	92.308
70	3.43	6.5	13.908	92.857
75	3.66	7	13.492	93.333
80	3.89	7.5	13.066	93.750

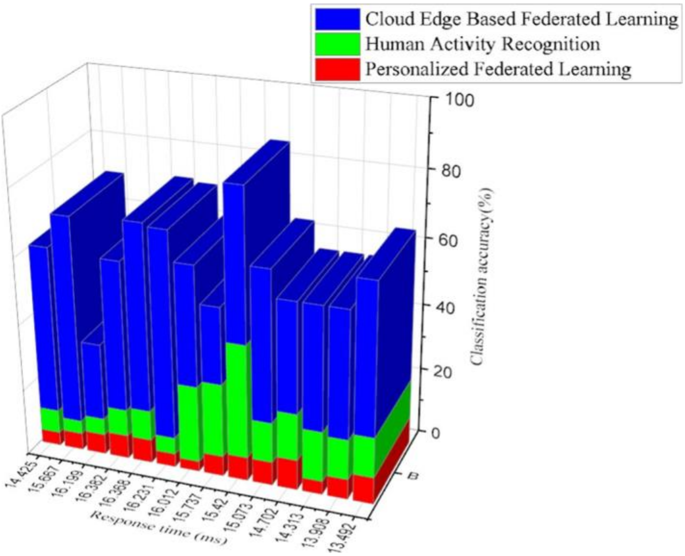


Fig. 7 Classification accuracy suspicious human finding

Table 3 Classification Accuracy both normal and patient finding versus Moving data object count and Response Time

Patient finding (Nos)	Data count (n)	Data rate (R)	Time (Sec)	Response time (ms)	Classification accuracy (%)
1	10	0.45	1.23	20.992	0.476
3	15	0.98	1.67	13.636	1.100
6	20	1.51	2.11	11.135	1.796
8	25	2.04	2.55	9.705	2.576
10	30	2.57	2.99	8.683	3.455
12	35	3.1	3.43	7.860	4.453
14	40	3.63	3.87	7.149	5.595
17	45	4.16	4.31	6.507	6.916
19	50	4.69	4.75	5.911	8.459
21	55	5.22	5.19	5.346	10.288
23	60	5.75	5.63	4.805	12.487
26	65	6.28	6.07	4.280	15.187
28	70	6.81	6.51	3.769	18.573
30	75	7.34	6.95	3.268	22.950
32	80	7.87	7.39	2.775	28.829

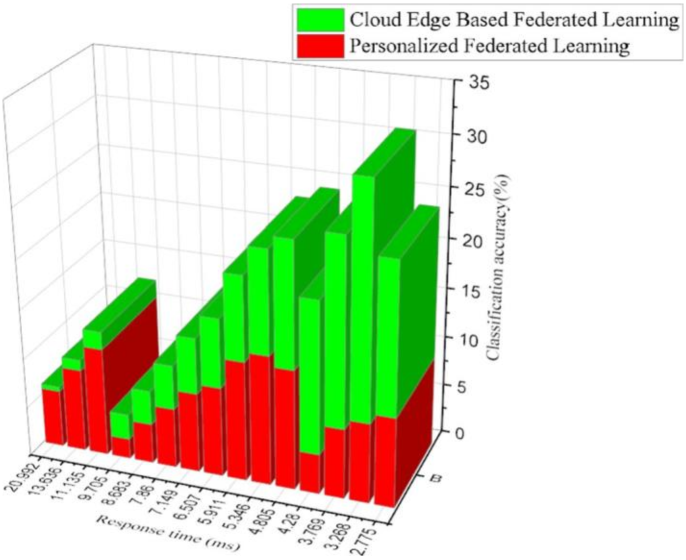


Fig. 8 Classification accuracy both normal and patient findings concerning response time

Moving data object count and Response Time; as an integral component of health care quality, patient experience includes several aspects of health care delivery that patients value highly when they seek and receive care, such as getting timely appointments, easy access to information, and good communication with health care providers. Response time is equal to n divided by r and minus t. n represents data count, r represents data rate, and t means time.

Above Fig. 8. Classification Accuracy of both standard and patient findings is based on object data and classification accuracy (Firouzi et al. 2020). This graph comparison result is compared to cloud-edge-based federated learning and personalized federated learning. Cloud-edge-based federated learning is 70.9% efficient. Table 4 shows

$$\text{Precision} = \frac{\text{the no of relevant document retrieved by a search engine}}{\text{the total no of documents retrieved by that search}} \tag{12}$$

Precision equals the number of the relevant documents retrieved by a search engine divided by the total number of records retrieved by that search.

$$\text{Recall} = \frac{\text{no of document retrieved by a search engine}}{\text{total no of relevant document available on the search}} \tag{13}$$

The Moving data object count and Response Time vs. Precision vs. recall are based on precision, recall, moving data object count, and response time. A memory equals the number of documents retrieved by a search engine divided by the total number of relevant documents available on the search. Response time is the whole time it takes to respond to a request for service (Kishor et al. 2021).

Table 4 The Moving data object count and Response Time versus Precision versus recall

No of the relevant Training document	No of the retrieved Testing document	No of the retrieved Training document	no of the relevant Testing document	Precision	Recall	Data count(n)	Response time (Sec)
3	2	2	1	0.020	0.025	10	0.67
8	6	4	4	0.060	0.009	20	0.9
13	10	6	7	0.100	0.005	30	1.13
18	14	8	10	0.140	0.004	40	1.36
23	18	10	13	0.180	0.003	50	1.59
28	22	12	16	0.220	0.003	60	1.82
33	26	14	19	0.260	0.002	70	2.05
38	30	16	22	0.300	0.002	80	2.28
43	34	18	25	0.340	0.002	90	2.51
48	38	20	28	0.380	0.002	100	2.74
53	42	22	31	0.420	0.001	110	2.97
58	46	24	34	0.460	0.001	120	3.2
63	50	26	37	0.500	0.001	130	3.43

Above Fig. 9, The Moving data object count and Response Time vs. Precision refer to how close measurements of the same item are to each other. Precision is independent of accuracy. This graph comparison result is cloud-edge based federated learning and personalized federated learning. The cloud-edge-based federated learning is 45.8% efficient. Training machine learning algorithms for several customers, every with a unique information dispersion, is the responsibility of personalized federated learning. The objective is to jointly develop tailored algorithms, compensate for information differences among customers, and lower transmission losses.

Above Fig. 10, The Moving data object count and Response Time vs. recall, recall is also used as a verb to request a person to return somewhere. This graph comparison result is compared to the proposed system of cloud-edge-based federated learning and the existing human activity recognition system (Kishor et al. 2021). The proposed method of cloud-edge-based federated learning is 52.3% efficient. Table 5 shows

$$\text{f - measure} - \frac{2 * (precision * recall)}{(precision + recall)} \tag{14}$$

f-measure is equal to 2 is multiplied by precision multiplied by the recall. These are divided by the sum of precision and recall. The Moving data object count and Response Time vs. F- Measure, The F-measure, also called the F1-score, measures a model's accuracy on a dataset. The F-score combines the precision and recall of the model, and it is defined as the harmonic mean of the model's precision and recall.

Above Fig. 11, F-measure is based on response time, data count, precision, and recall. Accuracy refers to how close measurements of the same item are to each

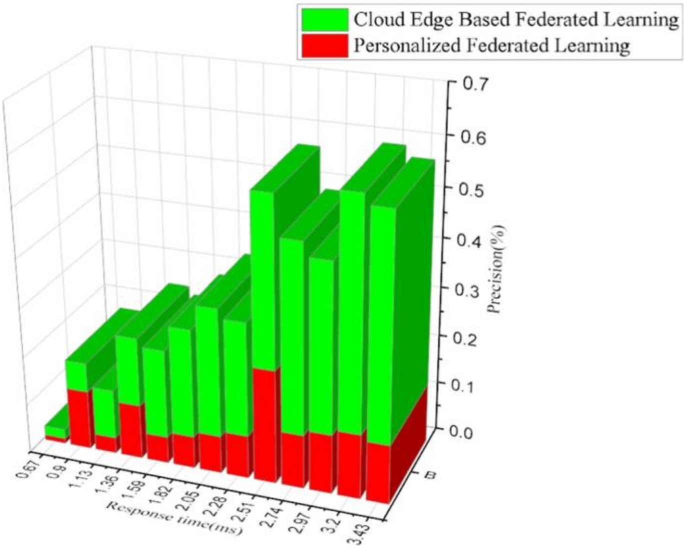


Fig. 9 The Moving data object count and response time versus precision

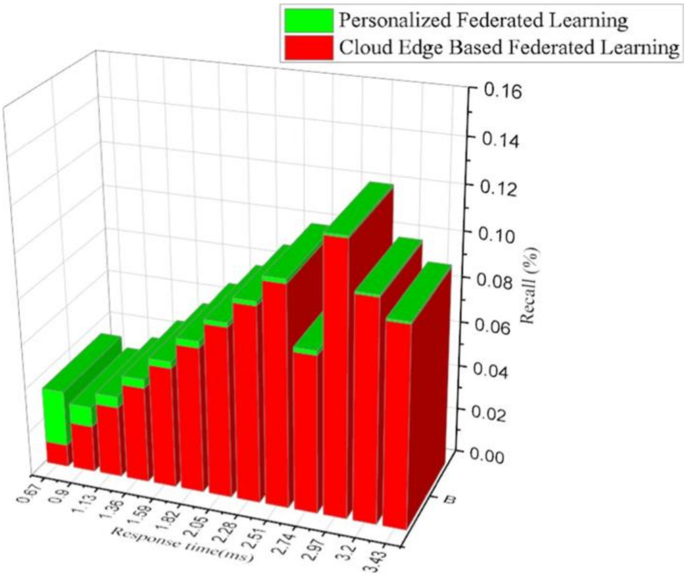


Fig. 10 The Moving data object count and response time versus recall

Table 5 The Moving data object count and Response Time versus F- Measure

Data count (n)	Response time (Sec)	Precision	Recall	f-measure
1	2.34	0.6	0.180	0.276923077
2	3.67	0.57	0.2	0.296103896
3	5.69	0.56	0.26	0.355121951
4	6.33	0.562	0.86	0.679774965
5	7.66	0.5607	0.28	0.373488759
6	8.99	0.56	0.12	0.197647059
7	10.32	0.559	0.29	0.38188457
8	11.65	0.558	0.544	0.550911071
9	12.98	0.558	0.299	0.389362894
10	14.31	0.55814	0.118	0.194813264
11	15.64	0.5578	0.30	0.390160877
12	16.97	0.5576	0.2202	0.315720031
13	18.3	0.5575	0.30	0.390087464
14	19.63	0.5573	0.256	0.350839297
15	20.96	0.5572	0.30	0.390013999

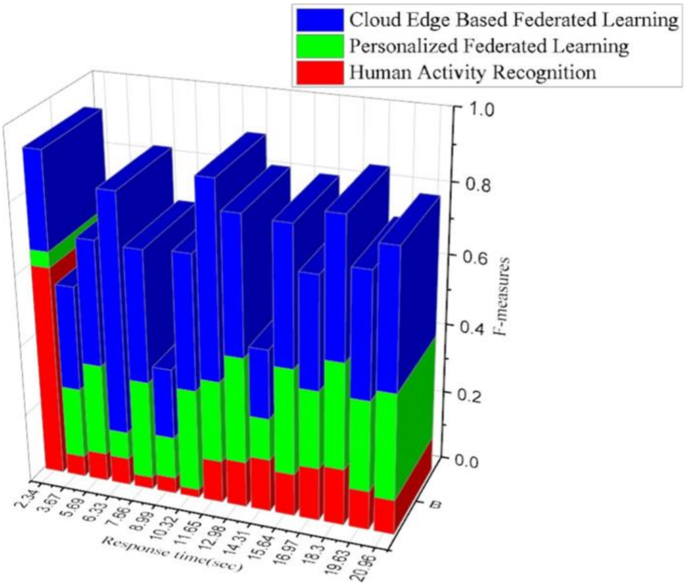


Fig. 11 F- Measure versus response time

Table 6 The Specificity versus Sensitivity based on Moving data object count and Response Time

Data count (n)	True positive (TP)	Total diseased (Count)	True negative (TN)	Total healthy (Count)	Sensitivity (%)	Specificity (%)	Response time (Sec)
10	2	1	3	4	33.3333	25	1.78
20	5	8	6	9	35.7143	57.1429	1.34
30	8	15	9	14	36.3636	62.5	1.9
40	11	22	12	19	36.6667	64.7059	2.46
50	14	29	15	24	36.8421	65.9091	3.02
60	17	36	18	29	36.9565	66.6667	3.58
70	20	43	21	34	37.037	67.1875	4.14
80	23	50	24	39	37.0968	67.5676	4.7
90	26	57	27	44	37.1429	67.8571	5.26
100	29	64	30	49	37.1795	68.0851	5.82
110	32	71	33	54	37.2093	68.2692	6.38
120	35	78	36	59	37.234	68.4211	6.94
130	38	85	39	64	37.2549	68.5484	7.5
140	41	92	42	69	37.2727	68.6567	8.06
150	44	99	45	74	37.2881	68.75	8.62

other. The recall is also used as a verb to request a person to return somewhere. The comparison result is that cloud-edge-based federated learning is 32.45% efficient (Wang et al. 2021). Table 6 shows

$$\text{Sensitivity} = \frac{TP}{\text{total diseased}} * 100 \tag{15}$$

Sensitivity equals true positive divided by the total diseased multiplied by a hundred. TP represents true positive.

$$\text{Specificity} = \frac{TN}{\text{total healthy}} * 100 \tag{16}$$

The Specificity Vs. Specificity equals true negative divided by the total healthy multiplied by a hundred. TN represents the actual negative. Sensitivity is based on Moving data object count and Response Time; object Counting is to count the number of object instances in a single image or video sequence (Srinivasa et al. 2018). Response time is the real-time it takes to respond to a request for service.

Above Fig. 12, Specificity is the quality of being precise and exact: There was a dramatic lack of specificity in his answer (Firouzi et al. 2020). Sensitivity is the quality of being tender, easily irritated, or sympathetic. This graph comparison result is cloud-edge based federated learning is 54.3% efficient. Table 7 shows

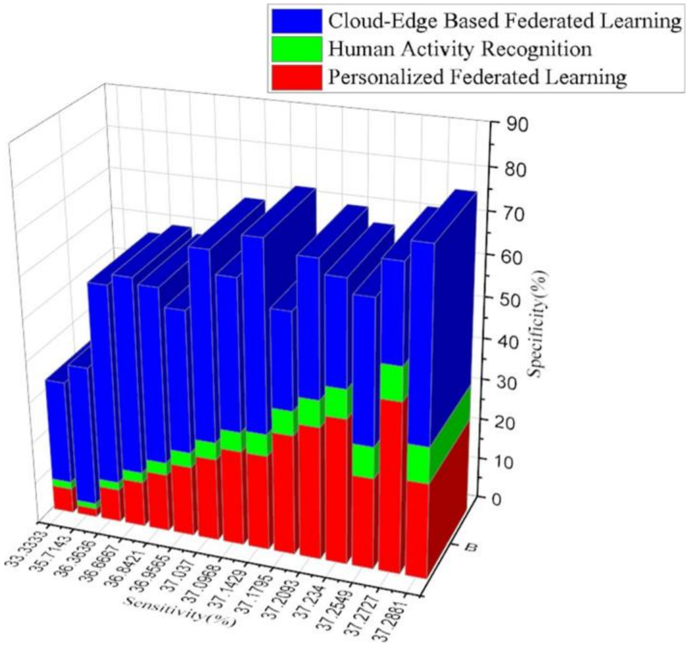


Fig. 12 Specificity versus sensitivity

Table 7 The Moving data object count and Response Time versus detection ratio

Time (Sec)	True positive (TP)	False-positive (FP)	Sum of true and false positive	Detection ratio (%)	Data count (n)	Response time (Sec)
2	3	2	5	10	5	1.55
4	5	7	12	8.3333	10	1.45
6	7	12	19	7.8947	15	2.35
8	9	17	26	7.6923	20	3.25
10	11	22	33	7.5758	25	4.15
12	13	27	40	7.5	30	5.05
14	15	32	47	7.4468	35	5.95
16	17	37	54	7.4074	40	6.85
18	19	42	61	7.377	45	7.75
20	21	47	68	7.3529	50	8.65
22	23	52	75	7.3333	55	9.55
24	25	57	82	7.3171	60	10.45
26	27	62	89	7.3034	65	11.35
28	29	67	96	7.2917	70	12.25
30	31	72	103	7.2816	75	13.15

$$\text{Detection ratio } = \frac{t}{N} * 100 \tag{17}$$

The detection ratio equals t divided by N, t represents time, and N represents the sum of true positive and false positive.

$$N = TP + FP \tag{18}$$

The Moving data object count and Response Time vs. detection ratio use a double-tuned transformer to convert the instantaneous frequency variations of the frequency input signal to fast amplitude variations. TP represents true positive, and FP represents false positive (Vermesan and Bacquet 2019). N is equal to the sum of true positive and false positive.

Above Fig. 13, This graph comparison result compares the proposed cloud-edge-based federated learning system and the existing personalized federated education system. The result is a proposed system of cloud-edge-based federated learning that is 75% efficient. Table 8 shows

$$\text{Coverage area} = \frac{\text{building area}}{\text{site area}} * 100 \tag{19}$$

The coverage area is the geographic region or location in which benefits of an insurance policy may apply and be applied to file a valid claim (Kishor et al. 2021). Coverage area equals building area divided by site area and multiplied by a hundred—-coverage area Vs. Classification Accuracy is based on Moving data object count and Response Time.

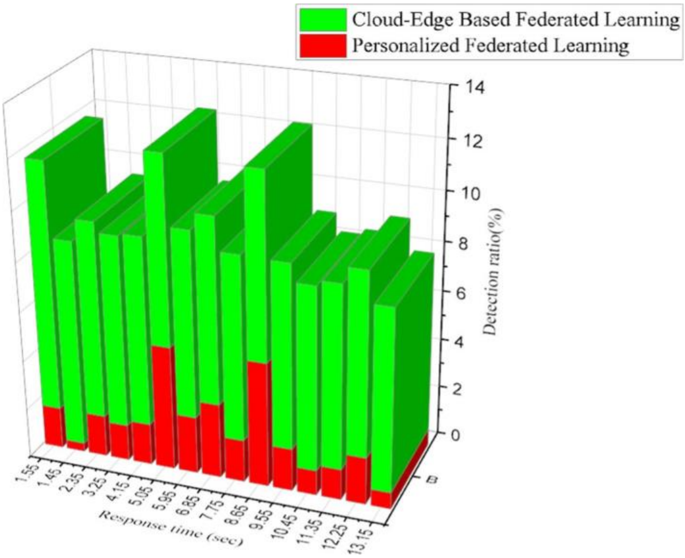


Fig. 13 Detection ratio versus response time

Table 8 Coverage area versus Classification Accuracy based on Moving data object count and Response Time

Building area (Sq.ft)	Site area (Sq.ft)	Coverage area (Sq.ft)	Data count	Response Time (Sec)	Classification accuracy (%)
3450	5320	6484.962	200	1.23	7.5
5200	7800	6666.667	400	1.78	15
6950	10,280	6760.7	600	1.33	22.5
8700	12,760	6818.182	800	1.88	30
10,450	15,240	6856.955	1000	2.43	37.5
12,200	17,720	6884.876	1200	2.98	45
13,950	20,200	6905.941	1400	3.53	52.5
15,700	22,680	6922.399	1600	4.08	60
17,450	25,160	6935.612	1800	4.63	67.5
19,200	27,640	6946.454	2000	5.18	75
20,950	30,120	6955.511	2200	5.73	82.5
22,700	32,600	6963.19	2400	6.28	90
24,450	35,080	6969.783	2600	6.83	97.5
26,200	37,560	6975.506	2800	7.38	91
27,950	40,040	6980.519	3000	7.93	97.5

Above Fig. 14, This graph is Coverage area Vs. Classification Accuracy, The classification accuracy ratio is the number of correct predictions to the total number of input samples. This graph comparison result is cloud-edge-based federated learning and is 68.7% efficient. Table 9 shows

$$\text{Sensing accuracy} = \frac{\underline{\text{actual participents} * \text{total participents count}}}{\text{data count}} - t* \quad 100 \tag{20}$$

The Moving data object count and Response Time are based on Sensing accuracy Vs. No of Participants, The sensor's accuracy is the maximum difference between the actual value and the indicated value at the sensor's output. Sensing accuracy is equal to the true value multiplied by a hundred.

Above Fig. 15, The Sensing Accuracy and number of Participants graph representation elaborate based on the number of participants and sensing accuracy. The result compares the proposed cloud-edge-based federated learning system and the existing personalized federated learning system. The comparison result shows that the cloud-edge-based federated learning system is 43.9% efficient.

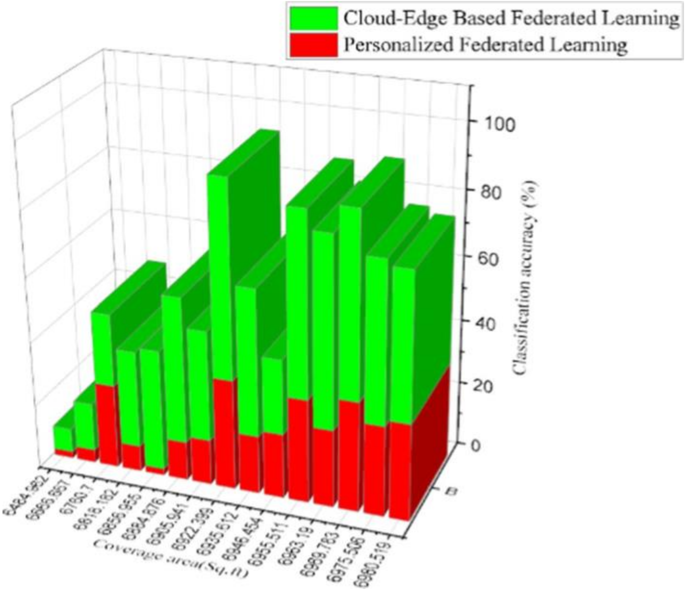


Fig. 14 Coverage area versus classification accuracy

Table 9 The Moving data object count and Response Time based on Sensing accuracy versus no of Participants

No of participant (Count)	Actual participant (Count)	Sensing Accuracy (%)	Data count (n)	Response time (Sec)
10	0.34	3.4	100	2.34
20	0.98	9.8	200	3.67
30	1.62	16.2	300	5
40	2.26	22.6	400	6.33
50	2.9	29	500	7.66
60	3.54	35.4	600	8.99
70	4.18	41.8	700	10.32
80	4.82	48.2	800	11.65
90	5.46	54.6	900	12.98
100	6.1	61	1000	14.31
110	6.74	67.4	1100	15.64
120	7.38	73.8	1200	16.97
130	8.02	80.2	1300	18.3
140	8.66	86.6	1400	19.63

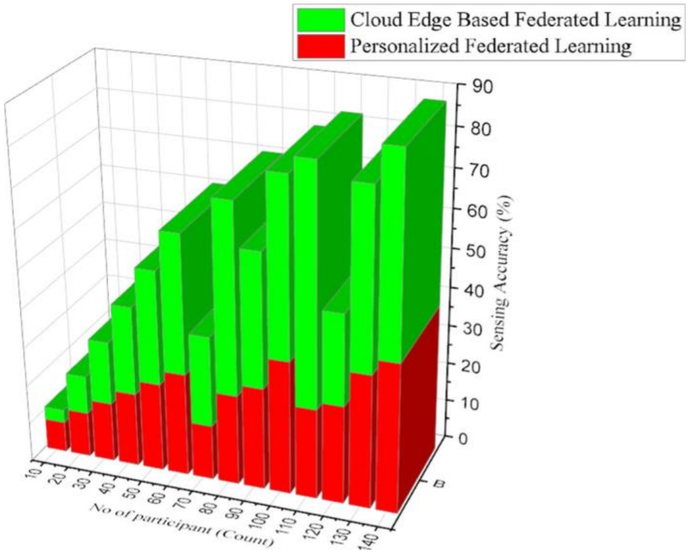


Fig. 15 Sensing accuracy versus number of participants

5 Conclusion

This research studies IoT for healthcare, intelligent and efficient maliciously roaming person features detection around hospital surface using cloud-edge based federated learning. The significance of cloud-edge-based federated knowledge in the internet of things, Hilbert spectrum, and cognitive dimensionality reduction under the grid computing platform is imposed. Grid computing is used in various concerns to solve many mathematical, analytical, and physical problems. In this paper, the different on-premises cloud-like or cloud edge-based architecture was discussed clearly. The general calculation of controller of IoT enabled drone explanation and camera with sensor facet is explained.

In suspicious person position estimation, the robust position estimation algorithm is obtained. The analysis of the prospered system has a greater accuracy of 92.5% with the moving data object count concerning the response time. The classification accuracy with the average human finding is 96.235% efficient. The classification accuracy of suspicious human results was significantly less. The average human finding classification accuracy is 14.21%, and the moving data object count and response time is 16.41%. The prediction value is 18.61% efficient for the patient count. Classification accuracy of suspicious human findings is 14.71%, and moving data object count and response time is 31.56%, the prediction value is 48.41% efficient for accuracy of questionable human results. Classification accuracy for both normal and patient findings is 22.45% and 46.2%, respectively; from this solution, the moving person count and response time is 69.95% efficient for authentic suspicious human results in intelligent cloud-edge-based federated learning. The specificity is increased from 0.335% to 0.365%. Meanwhile, the sensitivity is increased from 0.372% to 0.339% based on moving person count and federated learning. The following results are embedded with the maliciously roaming person's detection from the research contribution.

Author'scontributions All Author are Contributed to the design and methodology of this study, the assessment of the outcomes and the writing of the manuscript.

Funding No funds, grants were received by any of the authors.

Data availability All data generated or analysed during this study are included in the manuscript.

Declarations

Conflict of interest There is no conflict of interest among the authors.

References

Ahmad I, Shahabuddin S, Kumar T, Okwuibe J, Gurtov A, Ylianttila M (2019) Security for 5G and beyond. IEEE Commun Surv Tutor 21(4):3682–3722

Alimi IA, Patel RK, Muga NJ, Pinto AN, Teixeira AL, Monteiro PP (2021) Towards enhanced mobile broadband communications: a tutorial on enabling technologies, design considerations, and prospects of 5g and beyond fixed wireless access networks. Appl Sci 11(21):10427

Firouzi F, Chakrabarty K, Nassif S (eds) (2020) Intelligent internet of things: from device to fog and cloud. Springer, Berlin

Gedeon J, Brandherm F, Egert R, Grube T, Mühlhäuser M (2019) What the fog? Edge computing revisited: promises, applications and future challenges. IEEE Access 7:152847–152878

Kishor A, Chakraborty C, Jeberson W (2021) Intelligent healthcare data segregation using fog computing with internet of things and machine learning. Int J Eng Syst Model Simul 12(2–3):188–194

Kumar PM, Gandhi U, Varatharajan R, Manogaran G, Vadivel T (2019) Intelligent face recognition and navigation system using neural learning for smart security in Internet of Things. Clust Comput 22(4):7733–7744

Naeem RZ, Bashir S, Amjad MF, Abbas H, Afzal H (2019) Fog computing in the internet of things: practical applications and future directions. Peer-to-Peer Netw Appl 12(5):1236–1262

Nguyen VL, Lin PC, Cheng BC, Hwang RH, Lin YD (2021) Security and privacy for 6G: a survey on future technologies and challenges. IEEE Commun Surv Tutor 23(4):2384–2428

Qayyum A, Ahmad K, Ahsan MA, Al-Fuqaha A, Qadir J (2021) Collaborative federated learning for healthcare: multi-modal covid-19 diagnosis at the edge. arXiv preprint arXiv:2101.07511

Raad H (2020) Fundamentals of IoT and wearable technology design. Wiley, New York

Sharma PK, Ghosh U, Cai L, He J (2021) Guest editorial: security, privacy, and trust analysis and service management for intelligent Internet of Things healthcare. IEEE Trans Industr Inf 18(3):1968–1970

Smys S, Raj JS (2019) Internet of things and big data analytics for health care with cloud computing. J Inf Technol 1(01):9–18

Srinivasa KG, Sowmya BJ, Shikhar A, Utkarsha R, Singh A (2018) Data analytics assisted internet of things towards building intelligent healthcare monitoring systems: IoT for healthcare. J Organ End User Comput JOEUC 30(4):83–103

Suresh A, Udendhran R, Balamurgan M, Varatharajan R (2019) A novel internet of things framework integrated with real time monitoring for intelligent healthcare environment. J Med Syst 43(6):1–10

Vermesan O, Bacquet J (eds) (2019) Next-generation Internet of Things: distributed intelligence at the edge and human machine-to-machine cooperation. River Publishers, Denmark

Vermesan O, Bahr R, Ottella M, Serrano M, Karlsen T, Wahlstrøm T, Gamba MT (2020) Internet of robotic things intelligent connectivity and platforms. Front Robot AI 7:104

Wang T, Liu Y, Zheng X, Dai HN, Jia W, Xie M (2021) Edge-based communication optimization for distributed federated learning. IEEE Trans Netw Sci Eng

Wu Q, He K, Chen X (2020a) Personalized federated learning for intelligent IoT applications: a cloud-edge based framework. IEEE Open J Comput Soc 1:35–44

Wu W, He L, Lin W, Mao R (2020b) Accelerating federated learning over reliability-agnostic clients in mobile edge computing systems. IEEE Trans Parallel Distrib Syst 32(7):1539–1551