



6G Wireless Communication Cyber Physical System Based Smart Healthcare Using Quantum Optimization with Machine Learning

Hemalatha Thanganadar¹ · Syed Mufassir Yaseen² · Surendra Kumar Shukla³ · Ankur Singh Bist⁴ · Shavkatov Navruzбек Shavkatovich⁵ · P. Vijayakumar⁶

Accepted: 6 May 2024

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2024

Abstract

The ground-breaking paradigm of artificial intelligence (AI) will provide universal access to sixth generation (6G) edge computing-based E-healthcare. Internet world, where people and their personal gadgets like laptops, wearables, and cell phones, play a major role in facilitating the healthcare environment, is home to the cyber physical system (CPS). When it comes to availability as well as integrity of CPSs, blackhole, greyhole assaults are among the most dangerous. Ineffective protection results from the present detection and mitigation techniques' frequent inability to distinguish between harmful and authorised activity. In this research the proposed model is based on 6G wireless communication network in smart healthcare system optimization and cyber physical system analysis. The smart healthcare data analysis and optimization is carried out using quantum dirichlet convolutional learning coyote foraging optimizer. Then the network CPS analysis is carried out using federated honeypot transfer decentralized authentication model. Experimental analysis is carried out in terms of mean average precision, training accuracy, F-1 score, convergence rate, end-end delay. Proposed technique network security of 96%, mean average precision (MAP) 97%, training accuracy of 95%, F-1 score 77%, convergence rate of 88%. Regarding the suggested predictive model for a health system, the experimental findings provide positive findings. As a result of suggested work, CPS employing a suggested model improves medical data security with a high accuracy rate.

Keywords 6G network · Wireless communication · Smart healthcare system · Cyber physical system · Optimization · Authentication model

1 Introduction

The remarkable and powerful characteristics of 6G communication technology have drawn attention of numerous researchers. These attributes are demonstrated by the technology's astounding revolutionary advancement in most fields, and it is anticipated to become obvious starting in 2030 [1]. Many nations have already started exciting 6G projects; from 2018 to the present, these include Finland, USA, China, South Korea, Japan. Additionally, academics

Extended author information available on the last page of the article

around the world have made major contributions and used a variety of scientific and technical approaches when studying 6G. This is all a result of the difficulties and immature platform presented by 5G in relation to contemporary lifestyles. These challenges include, for instance, business and societal demands that are less receptive to holographic communication at lower data rates as well as intelligent patient monitoring and provisioning. Two main factors influencing the equitable distribution of resources in delicate and valuable healthcare scenarios are AI and 6G. Sensors, actuators, connectors, and other components, IoT has dramatically transformed healthcare industry as well as paved way for CPS [2]. Because of its centralised nature, the new internet paradigm is insufficient to cover the majority of application space. Because of the profound effects that CPSs have on society, the economy, and the environment, CPSs have garnered interest from academics, industry, and government. Interest in CPSs has increased recently due to the field's potential to benefit society, economy, environment, individual citizens. More significantly, quick developments in computer, communication, storage methods have led to domination as well as innovation in data transmission methods [3]. The next generation of integrated communications, computer, management systems is referred to as CPS, however a precise term is lacking. These systems strive to reach strength, efficiency, and dependability when it comes to biological data. Simultaneously, research endeavours undertaken to accomplish these goals primarily concentrate on attaining security within CPS. Any breaches in the security of these networks could have disastrous consequences due to the extensive integration of CPS in numerous critical infrastructures [4]. An accident could happen, for instance, if there is a communication system breakdown between the cars and inaccurate distance information is transmitted. In fact, arrival of autonomous vehicles has made matters substantially worse, since consumers now depend on all available automobile choices [5]. Confidentiality of CPSs is a significant issue in addition to security worries. Cyber-physical systems often span large geographic distances as well as produce massive amounts of data that are needed for data analysis and decision-making. By gathering data, system can use sophisticated algorithms to make judgement calls. Moreover, data theft can happen in any part of the system, including the phases of data gathering, video streaming, processing, and backup. Once more, a lot of the CPS design methods used today do not take data security into account, endangering the data that is collected. In order to arrive at the optimum judgement, cutting-edge methods like AI, machine learning (ML), deep reinforcement learning (DRL) can be used to do best analysis of the vast data. The aforementioned methods can result in best or almost optimal control decisions by taking a long-term goal into account. By strengthening learning capacities and consequently automated decision efficiency of the previously described strategies, the amount of training data may be increased to further improve the accuracy and precision of these methods. In addition to traditional intrusion detection systems (IDS) techniques, CPS security researchers are examining novel approaches to detection and mitigation, including deep learning (DL) and AI. But it's important that detection is not enough; suitable mitigation measures also need to be put in place in order to respond to attacks that are detected and decrease their impact on CPSs [6].

2 Related Works

The purpose of this section is to provide the general public with a safe solution by cataloguing and contrasting various scholarly articles according to their unique focuses and traits. In preparation for the impending 6G networks, the authors of [7] outline the concepts and potential of single- and multi-agent DRL frameworks. For IoT applications [8],

provides a comprehensive overview of DRL algorithms. For many Internet of Things (IoT) applications, such as smart grids, intelligent transportation systems, and industrial IoT applications, the pros and cons of using DRL algorithms are investigated. In [9], the authors summarise the latest research on the use of DRL in AIoT solutions and provide a general paradigm for AIoT systems. A number of recent studies have highlighted machine learning algorithms, and more especially reinforcement learning algorithms, as a potentially game-changing strategy for Internet of Things security. To defend Internet of Things (IoT) devices from different types of threats, RL is really gaining popularity. The authors of [10] summarise several RL-based security approaches that have been proposed in the literature for protecting IoT devices while reviewing numerous forms of cyberattacks in IoT networks. Authors in [11] adopted the concept of solar energy harvesting in BSN to build unique QoS-oriented algorithms, however power management from various angles is not main focus. Integrated power as well as energy harvesting technique for equitable resource allocation in BSN as well as healthcare was created by researchers in [12], but they did not address appropriate power conservation in BSN. Hybrid gearbox control as well as battery charge-aware algorithms were created by the authors in [13], CPS driven **E-healthcare** application is not covered in their work. In order to present power management methods for green as well as smart healthcare, researchers in [14] summarised their work in developing duty-cycle management-based charge optimisation in BSN. Researchers in [15] created dynamic power control techniques for wireless networks as well as WSNs, including a TPC-based strategy for energy optimisation. The authors of [16] did not focus on power management techniques in BSNs, but instead looked at and optimised the effects of TPC energy as well as lifetime of WSNs and WPT methods. The authors of [17] created wireless power transfer networks, TPC-based methods for cognitive radio, resource allocation; however, they did not concentrate on power management for intelligent healthcare in their work. MAC layer based QoS aware energy efficient strategy was created by the authors in [18], however they did not take fair power allocation and management strategies into account. Aside from the vocal pathology detection, no other illness prediction mechanism is included in this paper. In context of remote healthcare, QoS concerns have been examined in [19]. The paper addresses the big data system for urban healthcare's QoS issues. Although it discusses issues with physical CPS systems and healthcare, it does not provide information on how IoT-sensor data might be intelligently analysed for NCD forecasts. The study in [20] does not indicate risk prediction of any specific disease, but the author suggests a CPS that incorporates localization information on the sensing, analysing, and sharing of patient data for continuous health monitoring. The work in [21] demonstrates a CPS implementation to monitor body temperature (BT), heart rate (HR), blood pressure (BP), and blood glucose (BG) based on embedded and cloud-based technology in the field of general healthcare monitoring. This system integrates the CPS's communication, processing, and control aspects to enable patients to be continuously monitored and, if needed, to get therapy remotely. The suggested solution enhances CPS security by preventing hostile nodes from interfering with network communication [22] has suggested a lightweight trust-enabled routing method to lessen effects of Sybil attacks on RPL-based IoT networks. Recommended technique improves security as well as dependability of IoT networks by effectively identifying and thwarting Sybil attacks. Contribution is a functional IDS solution that has been adjusted based on RPL to meet the unique requirements and characteristics of IoT networks. Work [23] offer a thorough summary of all the routing attacks and defences using RPL control messages.

Everyone will have access to E-healthcare based on 6G edge computing as a result of the major paradigm change in AI. The availability and integrity of CPSs are particularly

vulnerable to blackhole and greyhole assaults. Inadequate security may occur when existing mitigation and detection systems cannot distinguish between harmful and permitted behaviours. In this research, we use a model based on 6G wireless networks to improve smart healthcare systems and perform cyber physical system evaluations. Data from smart healthcare systems may be analysed and optimised using the Quantum Dirichlet Convolutional Learning Coyote Foraging Optimizer. The next step is to analyse the network's CPS using the federated honeypot transfer decentralised authentication technique.

3 Smart Healthcare Data Analysis and Optimization Using Quantum Dirichlet Convolutional Learning Coyote Foraging Optimizer (QDCL-CFO)

Figure 1 describes the general configuration of the smart healthcare CPS. Because the attackers attempt to exploit the integrated environment, CPSs are vulnerable to these kinds of attacks. Unauthorised access to a CPS puts the system at risk of hostile actors penetrating the network and causing performance issues. Similar to this, manipulating data can undermine the integrity of the system and fool its decision-making processes. Furthermore, ransomware, viruses, and malware interfere with CPSs' normal operations. As a result, these attacks may have disastrous effects, such as bodily injury, monetary losses, and occasionally even fatalities. Attacks on CPSs, particularly blackhole as well as greyhole attacks, pose a serious threat to smart healthcare CPSs.

Every characteristic in QDCL can be expressed as a quantum bit (Q-bit(q)), where q represents the binary value superposition (0, 1). Resulting formula is utilized to develop mathematical model Q-bit(q) by Eq. (1).

$$q = \alpha + i\beta = e^{i\theta}, |\alpha|^2 + |\beta|^2 \quad (1)$$

where, probability values of 0 and 1 for the Q-bit are represented by the respective symbols α and β . The angle of q is indicated by the θ parameter and is increased by $\tan^{-1}(\alpha/\beta)$. Finding change in value of q is main objective of QDCL, which may be stated as follows by Eq. (2).

$$q(t+1) = q(t) \times R(\Delta\theta) = [\alpha(t)\beta(t)] \times R(\Delta\theta) \quad (2)$$

$$R(\Delta\theta) = \begin{bmatrix} \cos(\Delta\theta) & -\sin(\Delta\theta) \\ \sin(\Delta\theta) & \cos(\Delta\theta) \end{bmatrix}$$

In Eq. (15), θ is rotational angle of i^{th} Q-bit of j^{th} Q-solution. QDCL was used to maximise capacity to identify best feasible answer while balancing the best possible exploitation and investigation of DMA. Thirty percent and seventy percent of the total data are respectively testing as well as training subsets of recently developed FS method, QDCL. Next, using the training instances, the fitness value for each population is assessed. Better agents are then assigned based on the minimum fitness value. The DCL algorithm's operator adopts the solution during the exploitation phase. Update each person in turn until halting condition is met. Testing set dimensionality was then reduced in accordance with the superior solution, several metrics were used to evaluate the applied QDCL as FS. First, the N agents that represent the population are created. There are D features and Q -bits in every solution. As a result, X_i in Eq. (16) is the formula for the solution, as stated below by Eq. (3).

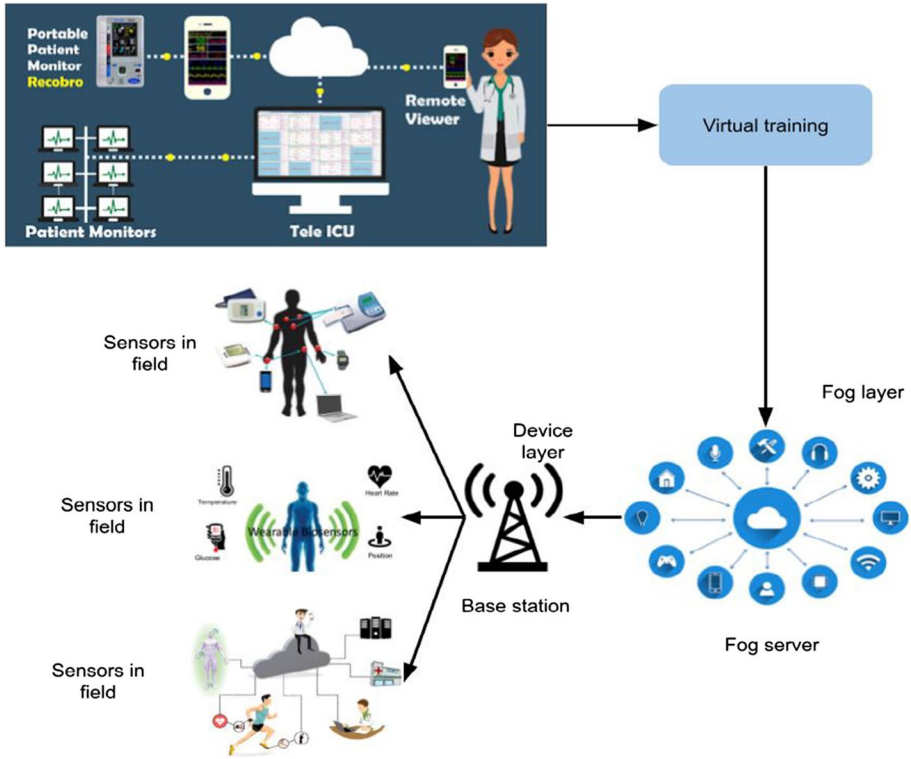


Fig. 1 CPS based smart healthcare in 6G network

$$X_i = [q_i | q_{i2}] \cdots | q_{iD} = [\theta_{i1} | \theta_{i2} \dots \theta_{iD}], i = 1, 2, \dots, N \tag{3}$$

The X_i represents a set of superpositions of probability for feature that are either selected or not. Updating agent till they reach the stopping condition is the main goal of this QDCL stage. The binary of each distinct X_i Eq. (4) to produce:

$$BX_j = \begin{cases} 1 & \text{if rand} < |\beta|^2 \\ 0 & \text{otherwise} \end{cases} \tag{4}$$

where, β is found using Eq. (5). The number created at random is indicated by $\text{rand} \in [0, 1]$. In the second stage, the classifiers are trained using the corresponding training feature from BX_{ij} , and the fitness values are computed as follows:

$$Fit_i = \rho \times \gamma + (1 - \rho) \times \left(\frac{|BX_{ij}|}{D} \right) \tag{5}$$

The variable $|BX_{ij}|$ in the preceding equation indicates total number of features selected, and γ shows error classification utilizing classifier (applicable feature). The factor that equalises the fitness values of the two sections is $\rho \in (0, 1)$. Gamma random variables can be used to replicate the Dirichlet distribution since

$\tilde{z}_{1:K} = \frac{z_{1:K}}{\sum_i z_i} \sim \text{Dirichlet}(\alpha_{1:K})$. This is significant because there is an effective rejection sampler for the gamma distribution by Eq. (6).

$$z = h_{\Gamma}(\epsilon, \alpha) := \left(\alpha - \frac{1}{3}\right) \left(1 + \frac{\epsilon}{\sqrt{9\alpha - 3}}\right)^3, \epsilon \sim N(0, 1) \tag{6}$$

However, because some samples are rejected, utilising this proposal function is not the same as employing a gamma distribution. Consequently, we require the distribution of an approved sample, denoted as $\epsilon \sim s(\epsilon)$, which is acquired through marginalisation over the rejection sampler’s uniform variable, u by Eq. (7).

$$\pi(\epsilon; \theta) = \int \pi(\epsilon, u; \theta) du = s(\epsilon) \frac{q(h(\epsilon, \theta))}{M_{\theta} r(h(\epsilon, \theta))} \tag{7}$$

where, $z = h(\epsilon, \theta)$, $\epsilon \sim s(\epsilon)$ is the reparameterization of the proposal distribution, M is a constant utilised in the rejection sampler, and r is the proposal function for the rejection sampler. This allows for the ELBO to be rewritten as Eq. (8).

$$\mathbb{E}_{q(z|x_i)}[-\log q(z | x_i)] + \mathbb{E}_{q(z|x_i)}[\log p(x_i, z)] = \mathbb{E}_{q(z|x_i)}[-\log q(z | x_i)] + \mathbb{E}_{\pi(\epsilon; \theta)}[\log p(x_i, h(\epsilon, \theta))] \tag{8}$$

After that, the gradient can be divided into three parts by Eq. (9).

$$\nabla_{\theta} \mathcal{L}(\theta) = g_{\text{rep}} + g_{\text{cor}} + \nabla_{\theta} \mathbb{E}_{q(z|x_i)}[-\log q(z|x_i)], \tag{9}$$

where, the values of g_{rep} and g_{cor} for a Monte Carlo estimator for a single sample are as follows by Eq. (10).

$$\begin{aligned} g_{\text{rep}} &= \nabla_z \log p(x_i, z) \nabla_{\theta} h(\epsilon, \theta) \\ g_{\text{cor}} &= \log p(x_i, z) \nabla_{\theta} \log \frac{q(h(\epsilon, \theta))}{r(h(\epsilon, \theta))} \end{aligned} \tag{10}$$

Hence, an analytical calculation of the entropy is possible. The gradient is represented by g_{rep} , which assumes that the proposal is accurate and always accepted, and g_{cor} , which represents a correction component of the gradient that takes into consideration proposals that are not exact.

As seen in Fig. 2, we suggested a comprehensive smart healthcare paradigm that included every element. Using smart sensor nodes positioned within or on top of the patient’s body, data is first gathered. These sensor nodes are additionally linked to mobile devices, gateways, and access points. Patients and medical personnel can communicate from anywhere, including the office or home, using mobile devices. These mobile communications can be handled by the complete cellular network. Significant security issues have been encountered in this activity due to the emergence of open networks. We suggest utilising a safe Android application to gather data and transfer it to the dependable cloud-based model. From this model, information is gathered, ML techniques are used to extract features, and a dynamic and accurate predictive model related to cardiovascular disease is presented. The three modules of the competing smart healthcare paradigm are depicted in Fig. 2.

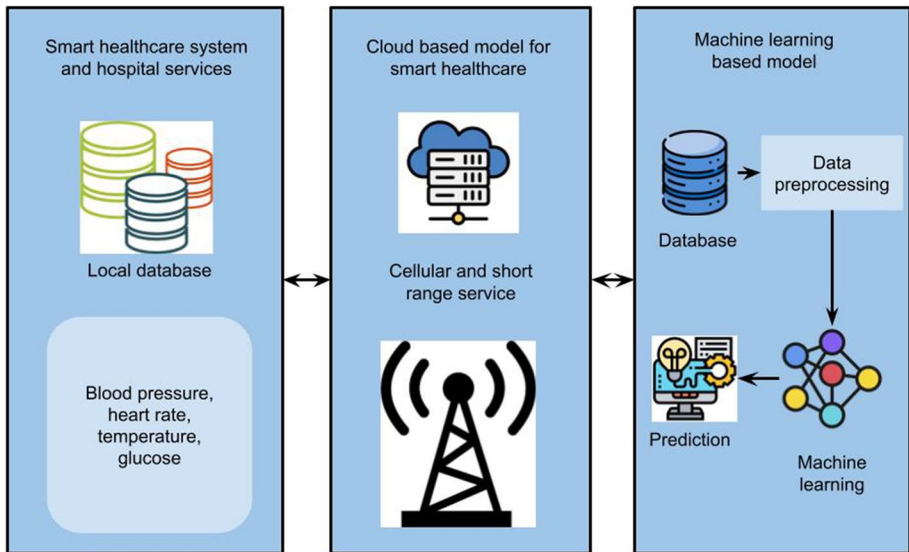


Fig. 2 smart healthcare model using machine learning technique

Convolution process is utilized to extract sentiment features from N-grams that filters convolved themselves with by running across entire input matrix. Here, g is a non-linear function; it's hyperbolic tangent. This is how a feature c_i is created by Eq. (11).

$$c_i = g(F * w_{i:i+h-1} + b) \quad (11)$$

Filtering process generates a feature with a size of $n-h+1$ for each input sentence. Feature maps are created by a set of filters; to extract most sensitive responses across 0.0 features, a pooling procedure is required. In this study, we extract features from various sentence perspectives by applying filters of varied sizes. Pooling: After that, the feature maps are sent to the layer responsible for pooling operations so that the best answers are combined while retaining the feature's sequential information. Using max-over-time pooling approach, we determine highest feature value (c_{\max}) on map C by Eq. (12).

$$c_{\max} = \max\{C\} = \max\{c_1, \dots, c_{n-h+1}\} \quad (12)$$

In order to accomplish population development, the bacterial foraging algorithm made advantage of its unique behaviours, such as chemotaxis, reproduction, and elimination-dispersal, to constantly update the locations of individual bacteria and locate optimal spots for groups of bacteria. Here we will go over the main steps of the algorithm that optimises bacterial foraging. Step 1 (initialization of parameters). N_{re} is the number of reproduction stages, N_{ed} is number of elimination-dispersal events. Number of chemotaxis stages is N_c . Fundamental probability of elimination-dispersal is called P_{ed} . Scale of bacteria is SS . Maximum number of chemotactic steps is denoted by N_s . Step 2: Determine the starting fitness values of the bacteria and initialise their locations. Step 3: Complete the circle of elimination and dissemination. Reproduction loop $k=1$: N_{re} , chemotaxis loop $j=1$: N_c , and $l=1$: N_{ed} . Step 4: Execute the chemotaxis loop of bacteria. Use $X_i(j, k, l)$ to express the bacteria's space location vector, where j denotes

chemotaxis loop's j th generation, k the reproduction loop's k th generation, and l the elimination-dispersal loop's l th generation. (1) Tumble. Update the locations of micro-organisms by Eq. (13).

$$X_i(j + 1, k, l) = X_i(j, k, l) + C(i) \times \phi(i, j)$$

$$\phi(i, j) = \frac{\Delta(i, j)}{\sqrt{\Delta^T(i, j)\Delta(i, j)}} \tag{13}$$

where, $C(i)$ is the bacteria i 's chemotaxis step length. When falling in the j th loop, Bacteriophage Γ 's normalised random direction vector is represented by $\phi(i, j)$. Each member of the randomly produced random direction vector $\Delta(i, j)$ is a random number on the interval $[-1, 1]$. (2) Proceed. It won't start to tumble if the tumbling fitness value rises until it either reaches the maximum number of steps, N_s , or it stops increasing. Step 5: Reproduction loop. Once chemotaxis loop is over, add together all of the fitness values that each bacteria has experienced throughout its life cycle to get an energy value. The bacteria should be sorted based on their energy values, and the half that cannot receive enough energy should be removed. Reproduce 50% of the bacteria that have a high capacity for energy absorption. The sixth step is the dispersal and elimination loop. Proceed with bacterium elimination-dispersal and random initialization in the solution space's defined domain if the produced probability is less than P_{ed} . Step 7: Find the loop's end condition. If it is met, stop loop and output results. One kind of *Canis latrans* is coyote. COA method balances the interaction between exploration and exploitation while solving optimisation challenges. Coyote packs hunt their prey. Every pack is led by an alpha male, crucial part of hunting strategy is infiltration. COA method defines population size as product of number of coyotes (N_c) in each pack and the number of packs (NP). These figures show potential fixes for the optimisation problem. First, the COA algorithm is used to randomly assign the coyotes to the packs. For the issue $U = (U_1, U_2, \dots, U_D)$, where D is issue dimension, each coyote represents a single solution. At beginning of procedure, each coyote has a random location solution, as shown in the Eq. (14) below:

$$U_{c,j}^{p,t} = lb_j + r_j \cdot (ub_j - lb_j) \tag{14}$$

where, $j \in (1, 2, \dots, D)$ and lb_j and ub_j denote the search space's lower and upper limits, respectively. A random number inside the interval $[0, 1]$ is the r_j . The following describes the coyote's ability to adapt to its surroundings and its fitness function by Eq. (15).

$$fit_c^{p,t} = f(U_c^{p,t}) \tag{15}$$

The alpha coyote of each pack, if the problem is one of minimization, is currently defined as follows by Eq. (16).

$$\alpha^{p,t} = \left\{ U_c^{p,t} \mid \arg_{c=\{1,2,\dots,N_c\}} \min(f(U_c^{p,t})) \right\} \tag{16}$$

Next, the following is an update to the coyote's new social status. $U_{c,j}^{p,t} = U_c^{p,t} + r_1 \cdot \delta_1 + r_2 \delta_2$, where δ_1 is separation between alpha male and any random coyote in pack and δ_2 is separation between a single coyote from the group and average position of all the coyotes in the pack. Within the range $[0, 1]$, the values r_1 and r_2 are randomly selected. Next, utilise the following equation to assess the new solution's fitness function and determine its capabilities by Eq. (17).

$$\text{newfit}_c^{p,t} = f(\text{new}_c^{p,t}) \quad (17)$$

The coyote makes the following decision regarding whether to maintain the new social condition or the old one by Eq. (19).

$$U_{c,j}^{p,t+1} = \begin{cases} \text{new}_c^{p,t}, & \text{newfit} \\ U_{c,j}^{p,t}, & \text{otherwise} \end{cases} \text{fit}_c^{p,t}, \quad (18)$$

Moreover, the COA algorithm takes into account a coyote's birth and death.

4 CPS Analysis Using Federated HoneyPot Transfer Decentralized Authentication Model

Minimising the total loss in relation to the local participant dataset is the aim of FL. Furthermore, the loss function at end device n for each local dataset Q_n is specified as Eq. (19).

$$F_n(\mathbf{w}) := \frac{1}{Q_n} \sum_{i \in Q_n} f_i(\mathbf{w}) + \zeta g(\mathbf{w}) \quad (19)$$

where, $g(\cdot)$ is a regularizer function, sometimes written as $g(\cdot)$, and $\mathbf{w} \in \mathbb{R}^d$ denotes the local model's parameters. This describes the local model in the FL context. The following global loss function minimization issue is then minimised by the learning model by Eq. (20).

$$\min_{\mathbf{w} \in \mathbb{R}^d} F(\mathbf{w}) := \sum_{n=1}^N \frac{Q_n}{Q} F_n(\mathbf{w}) \quad (20)$$

The first step for a dynamic honeypot server is to gather data, either actively or passively, on the hosts that are accessible on the networks. Depending on the network design, the administrator can decide which method of data collection is preferable to utilise. In order to avoid creating probing packets on the shared medium, administrator would run the dynamic honeypot server in passive mode if network is made up of machines connected through a hub where packet sniffing is possible. Passive fingerprinting would not be as trustworthy as active probing if network is a switched network with hosts connected to layer two switches. After getting a full image of the network, including the operating systems and services of the hosts, the dynamic honeypot server decides on the identities and features of the fake computers to be deployed. After that, it gives honeyd the proper setup parameters so that systems can be installed on network. This will allow both authentic as well as fraudulent methods to coexist on the network. The connections established to the fictitious systems—which are not operational methods as well as are not intended to receive network traffic—can be used to identify an intrusive party. It evaluates the relationship on the basis of consistency and resemblance. The difference or relative entropy in data or data related by 2 distributions during data transmission is measured using Kullback–Leibler (KL) divergence. The uniform distribution or probability of the data is evaluated using the KL divergence. The two most popular transfer learning methods in DL are deep feature extraction and fine-tuning. Pre-trained network receives input data and uses activation values of various layers to store and extract features throughout the deep feature extraction process. In the process of fine-tuning, a deep neural network is trained on a comparable problem where labelling is comparatively simpler. The latter layers of method

is fine-tuned to learn characteristics of new dataset, while initial layers of pre-trained network is fixed. Pre-trained method is retrained using fresh tiny dataset, its weight values are modified in accordance with the demands of the fresh task. Back-propagation with labels is used in the network to fine-tune the system. Because all parameters of a new NN are not estimated from scratch, learning to transmit is frequently faster than training a new neural network. More universal features, such colour blobs and Gabor filters, are present in the lower levels of the network and can be applied to different tasks. Higher layers, however, have additional task-specific properties. Deep learning systems perform well on a variety of tasks, but their training takes a very long time and a vast amount of data. Reusing these previously trained methods for related tasks is beneficial in this situation. Here are 15 layers in this CNN method. Image input layer is initial layer. One hundred by one hundred pixel images are supplied as input. The CNN method first resizes the leaf pictures that have varying widths and heights. Our network consists of three convolution layers. Primary layers of a CNN are called convolution layers. Filters to learn various feature types are present in these layers. Convolution is applied after each filter is slid over input images. Output is transferred to computed results of convolution processes. ReLu layers and batch normalisation layers come after a convolution layer. Activation values calculated by preceding layers are adjusted and normalised using batch normalisation layers. ReLu layers apply a threshold operation to input to remove influence of areas that are noisy and dark. Reducing the input dimensions is the responsibility of max-pooling layers in order to minimise computational complexity. Filter-corresponding values are subjected to a mathematical MAX operation in order to accomplish this process. The last levels in a CNN model are the completely connected layers. These layers are analogous to the layers found in CNN. These layers compute the class values for a given input. Each of these layers' activation values corresponds to a distinct abstraction layer. The top layers are the classification and softmax layers. The classification layer chooses the label with the highest likelihood as its output after the softmax layer applies the softmax algorithm.

5 Results and Discussion

Version 3.1 of the programme was utilized to test individual monitoring scenarios. Three open-source broker software tools were deployed and used on virtual computers. Oracle Virtual Box (Oracle, 2018) housed three virtual machines (VMs) on a Windows 10 PC to implement broker software. Each virtual system had a 15GB hard drive, 8GB of RAM, and one CPU set up. Utilising 13-class and binary classification, we evaluated our suggested model in order to comprehend the detection and tractable predictability of various threats and cyberattack models. To assess detection accuracy, however, we took privacy, data availability, and heterogeneity into account using a centralised multi-source transfer learning model. Rich data made available through centralised learning increases the likelihood of detecting unknown large-scale threats.

For a certain patient, each record in table is referred to as a ring. With a straightforward user interface, patient can generate an infinite number of static, unique rings for various files. Using index value, a patient can concurrently create a dynamic ring to accept valid file access requests from remote site. Patient establishes a unique index value for every file type based on pertinent data. The recommended matches requester's index value with ring's required index value to grant remote actors secure read-only access. For dynamic file access control, every hospital calculates values of local actors

index. The system stops uninvited actors from accessing files. While dynamic rings are helpful in managing requests for remote locations, static rings are utilised for access control services at hospital level.

Dataset description: We offer an analysis of the suggested architecture's performance. To assess the effectiveness of the suggested work, two widely available standard datasets with a range of feature characteristics, including continuous and categorical, are chosen for inclusion in the experimental research: the Power System dataset and the industrial UNSW-NB15, ISCX dataset. 37 scenarios with multiclass categories—normal activities (8), meddling actions (28) no actions (1)—are included in Power System dataset. Both current normal and attack records are included in industrial-based UNSW-NB15 dataset. This dataset comprises ten distinct classes—one class indicates normal, other nine distinct classes specify security events, moves between various network hops at a speed of between five and ten megabits per second in order to accurately replicate real-world network environments.

Because it was primarily used for 2014 UTHealth de-identification competition, i2b2 dataset serves as the baseline. Conversely, computer-assisted de-identification was applied to either Nursing Note or MIMIC-III. There were raw EHRs in the Nursing Note collection as well. We generated the labelled dataset by mapping both the raw and de-identified EHRs. Sadly, there were no raw EHRs in the MIMIC-III dataset that might have been utilised to build a dataset in a manner akin to what we accomplished for the Nursing Note. The dataset was developed by us by manually identifying and labelling the pseudo-PHI cases that were previously available in the MIMIC-III dataset. There might be certain edge instances in this approach where the size of the corpus prevents us from manually intervening. Nevertheless, we validated our results over a broader corpus using the Nursing Note dataset. These datasets are divided into three parts: train, test, and valid set.

Datalink for Clinical Practice Research (CPRD) General practitioners (GPs) are the primary point of contact for healthcare in the UK National Health Service, and over 98% of population is registered with one. Deidentified longitudinal primary care data is supplied to the CPRD service by a network of UK general practitioners. This data is then linked to administrative databases for area-based health care, secondary care, and other services. A few examples of these interconnected databases include Public Health England, the Index of Multiple Deprivation, Hospital Episode Statistics, and the Office of National Statistics. Approximately 10% of GP units provide CPRD with data. CPRD is one of the largest primary care EHR databases in the world, and it now enrolls patients from 674 GP units, accounting for 10 million of the 35 million patient lives that have been covered.

The original DARPA dataset, which reported on around 5 million suspicious activity evaluations within seven weeks of network traffic, is where KDD CUP (Knowledge Discovery and Data Mining) dataset began. This dataset represents an upgraded version of the IDS assessment, which is spearheaded by Massachusetts Institute of Technology's Lincoln Laboratory, to differentiate between legitimate as well as malevolent attack networks (MIT). There are forty-one basic, transit, and content feature classes in all. Additionally, attacks are classified according to their R2L (Remote to Local), U2R (User to Root), DoS (Denial of Service), and probing capabilities. For past 20 years, it is widely utilized dataset to assess IDS methods as well as most effective errors. Dataset's drawbacks include its age, the unpredictability of the test and training sets, the maximum number of twisted targets, inadequate features, and redundant patterns. To address shortcomings of KDD dataset, NSLKDD datasets were created. This dataset was improved, redundant-free, and more stable than KDD. The records are logical, precise, and organised as percentages. However, the lack of low footprint assault detection means that this dataset is still constrained.

Fig. 3 Simulation results based on execution time and cache hit rate

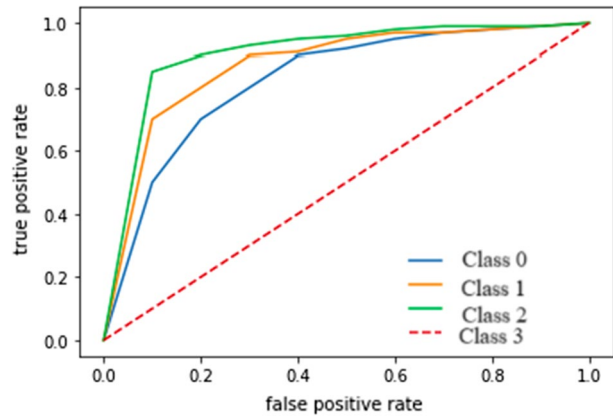


Table 1 Comparative for various smart healthcare dataset

Dataset	Techniques	Training Accuracy	Mean average Precision (MAP)	Convergence rate	Network security	F-1 score
UNSW-NB15	SVM	78	89	79	69	71
	RF-CNN	85	94	84	75	73
	QDCL-CFO	88	96	89	89	75
KDD CUP	SVM	92	88	88	90	84
	RF-CNN	94	93	92	95	86
	QDCL-CFO	96	97	95	98	88
i2b2	SVM	81	73	88	71	75
	RF-CNN	88	75	94	75	78
	QDCL-CFO	89	77	98	77	81
CPRD	SVM	92	81	90	79	79
	RF-CNN	94	85	96	80	81
	QDCL-CFO	95	88	99	81	85
ISCX	SVM	88	92	89	86	89
	RF-CNN	92	94	92	88	92
	QDCL-CFO	94	96	93	90	94

Simulation results based on true positive rate and false positive rate are shown in Fig. 3. Based on TP and TN, we divided the IoT data into various kinds.

The comparison for several smart healthcare datasets is shown in Table 1. With respect to network security, MAP, training accuracy, F-1 score, and convergence rate, the datasets examined here include i2b2, UNSW-NB15, ISCX, CPRD, and KDD CUP.

Cloud services were accessible as needed. Three common statistics were computed in order to evaluate the prediction models. The system made use of the lambda architecture, which is built on top of the Apache Kafka and Spark simulation tools; the hyper-parameters were set manually, but the model parameters were automatically evaluated based on the internal structure and validated based on the data. Prioritising communication latency is the first step in assessing a system's effectiveness. Efficacy, computer effectiveness, and half-total error rates of the suggested prediction models were

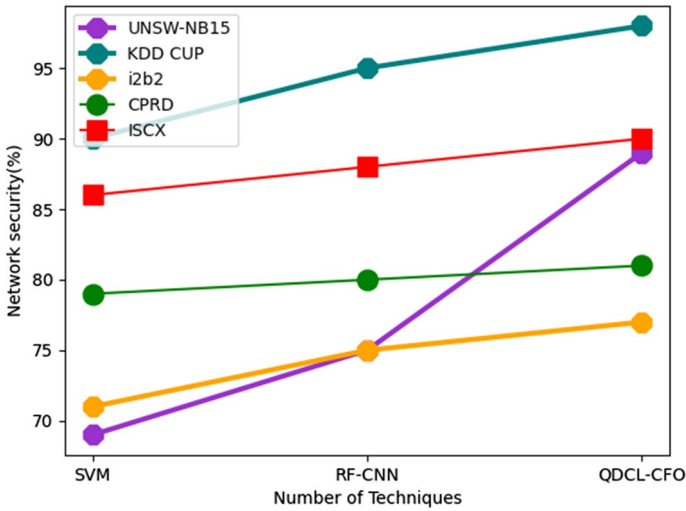


Fig. 4 Comparison of Network Security

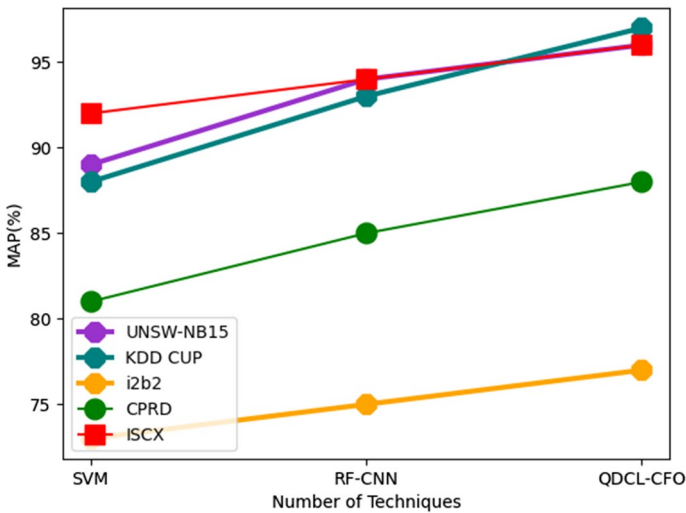


Fig. 5 Comparison of MAP

evaluated. The proposed technique obtained network security of 98%, as shown in Fig. 4, network security of 93% as shown in Fig. 5, for i2b2 dataset, proposed technique training accuracy of 98%, MAP 96%, convergence rate of 89%, network security of 89%; existing SVM training accuracy of 88%, MAP 89%, convergence rate of 79%, network security of 69%; CNN training accuracy of 94%, MAP 94%, convergence rate 84%, network security 75%. Figure 5 displays comparison analysis for CPRD dataset. Based on data presented in Fig. 6, proposed technique 99% training accuracy, 97% MAP, 95% convergence rate, 98% network security. In contrast, existing SVM 90% training accuracy, 88% MAP, 98% convergence rate, 90% network security. CNN 96%

training accuracy, 93% MAP, 92% convergence rate, 95% network security. Here, the suggested method achieved MAP of 89%, convergence rate of 93%, and network security of 85%. For the DARPA 98 dataset, existing CNN achieved mean average precision of 85%, convergence rate of 88%, network security 81%, while LSTM MAP of 88%, convergence rate 91%, network security 83%. Proposed technique achieved 90% MAP, 94% convergence rate, 88% network security for the KDD99 dataset. In contrast, existing CNN achieved 86% MAP, 89% convergence rate, 82% network security, while LSTM achieved 88% MAP, 92% convergence rate, 86% network security. The proposed method achieved 92% mean average precision, 95% convergence rate, 89% network security. For the UNSW-NB15 dataset, existing CNN achieved 87% MAP, 91% convergence rate, 85% network security, while LSTM, 89% MAP, 93% convergence rate, and 88% network security. The proposed technique MAP of 94%, convergence rate of 96%, and network security of 93% for ISCX dataset shown in Fig. 7. In contrast, the existing CNN achieved MAP of 88%, convergence rate of 92%, network security 89%, while LSTM achieved MAP of 92%, convergence rate 94%, network security 92%.

This is indicated by the values of accuracy, precision, and recall. It should be applied and then modified for use in more intricate and real-world systems that gather a greater amount of data, generating a greater number of periods, and varying parameters like the number of steps, the interval between steps, number of iterations, anything else that can enhance method in accordance with method it interfaces. Applying suggested method requires researching and modelling the infrastructure that it will be used on. Feedback from more impressive infrastructures, most importantly, from a practical method is needed for the data gathered in this effort. It should be examined how requests in bytes are categorised into ranges based on kinds of resources available in method. Since model would now contain categorised values rather than the requests' normalised values, this could help it learn even more quickly. It is also possible to change the model's implemented solutions, which include the number of hidden layers, features, hidden units, steps, time intervals, iterations, epochs, batch size, loss function, optimizer, and so on (Fig. 8).

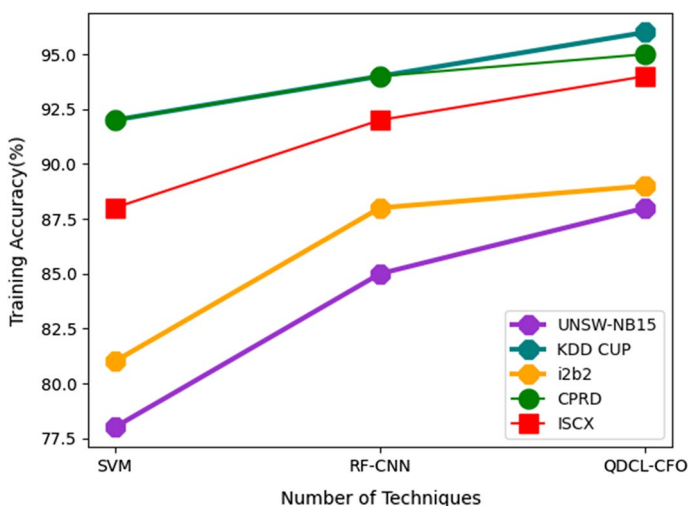


Fig. 6 Comparison of training accuracy

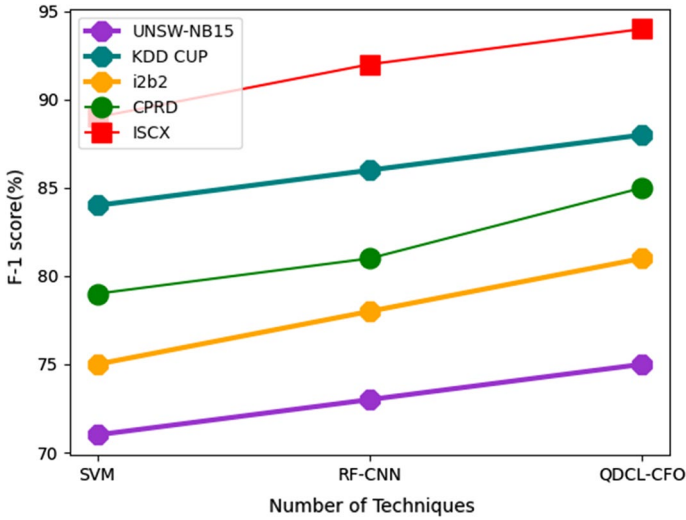


Fig. 7 Comparison of F-1 score

6 Conclusion

The proposed model in this study is based on a 6G wireless communication network for cyberphysical system analysis and smart healthcare system optimisation. Quantum Dirichlet Convolutional Learning Coyote Foraging Optimizer is used for the study and optimisation of smart healthcare data. Then, federated honeypot transfer decentralised authentication model is used to perform the network CPS analysis. This proposed model primarily takes into account the centralised mode when assessing different machine learning-based

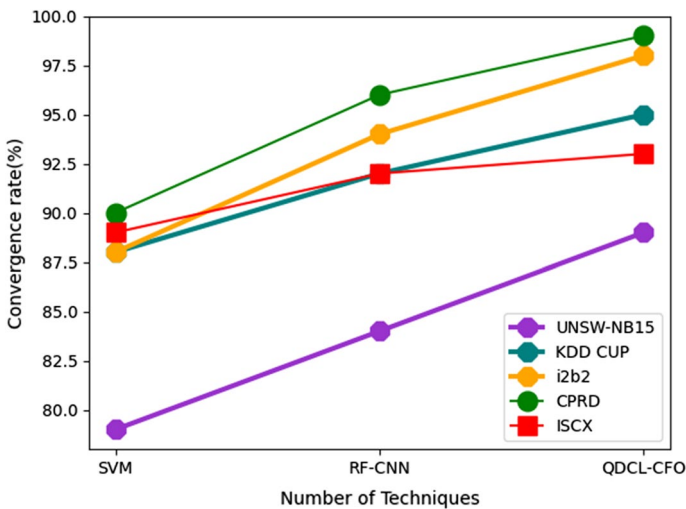


Fig. 8 Comparison of convergence rate

intrusion detection systems. The classifier development time with training data drops dramatically to 0.01 s since properly refined training data is used. Furthermore, the accuracy comparison with other previous research shows that the suggested framework outperforms the others for the majority of the classification algorithms taken into consideration. Without utilising the cloud, the suggested traditional teaching model successfully lowers latency decisions. Additionally, it was demonstrated that 3 bio-modalities evaluated in this article may provide a high degree of computation complexity and precision. Our intention is to explore use of compact DNN for fast performance in bio-modality fictitious classification tasks, where our model will be used. But at moment, data size is restricted to a specific length. Numerous security issues are exposed when contrasting the suggested system with the existing ones. Good accuracy is provided by the recommended system, indicating a positive assessment of performance component. Results are preserved by means of block-chain technology, which carries over properties like immutability, transparency, crypto hash-based connectivity.

Author Contributions 1. Hemalatha Thanganadar: Conceptualization, Methodology, Writing—Original Draft. 2. Syed Mufassir Yaseen: Data curation, Formal analysis, Writing—Review & Editing. 3. Surendra Kumar Shukla: Software, Visualization, Investigation. 4. Ankur Singh Bist: Validation, Resources, Writing—Review & Editing. 5. Shavkatov Navruzbek Shavkatovich: Supervision, Project administration, Funding acquisition. 6. Vijayakumar P: Supervision, Writing—Review & Editing, Funding acquisition.

Funding The authors have not disclosed any funding.

Data and materials availability All the data's available in the manuscript.

Declarations

Conflict of interest The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Ethical Approval This article does not contain any studies with animals performed by any of the authors.

References

1. Basu, D., Ghosh, U., & Datta, R. (2022). 6G for Industry 5.0 and smart CPS: a journey from challenging hindrance to opportunistic future. In *2022 IEEE Silchar Subsection Conference (SILCON)* (pp. 1–6). IEEE.
2. Jawad, A. T., Maaloul, R., & Chaari, L. (2023). A comprehensive survey on 6G and beyond: Enabling technologies, opportunities of machine learning and challenges. *Computer Networks*, *237*, 110085.
3. Hermawan, D., Putri, N. M. D. K., & Kartanto, L. (2022). Cyber physical system based smart healthcare system with federated deep learning architectures with data analytics. *International Journal of Communication Networks and Information Security*, *14*(2), 222–233.
4. Pattepu, S., Mukherjee, A., Routray, S., Mukherjee, P., Qi, Y., & Datta, A. (2023). Multi-antenna relay based cyber-physical systems in smart-healthcare NTN: An explainable AI approach. *Cluster Computing*, *26*(4), 2259–2269.
5. Peng, K., Liu, P., Bilal, M., Xu, X., & Prezioso, E. (2022). Mobility and privacy-aware offloading of AR applications for healthcare cyber-physical systems in edge computing. *IEEE Transactions on Network Science and Engineering*. <https://doi.org/10.1109/TNSE.2022.3185092>
6. Nauman, A., Nguyen, T. N., Qadri, Y. A., Nain, Z., Cengiz, K., & Kim, S. W. (2022). Artificial intelligence in beyond 5G and 6G reliable communications. *IEEE Internet of Things Magazine*, *5*(1), 73–78.

7. Kim, M., Oh, I., Yim, K., Sahlabadi, M., & Shukur, Z. (2023). Security of 6G enabled vehicle-to-everything communication in emerging federated learning and blockchain technologies. *IEEE Access*. <https://doi.org/10.1109/ACCESS.2023.3348409>
8. Ghildiyal, Y., Singh, R., Alkhayyat, A., Gehlot, A., Malik, P., Sharma, R., & Alkwa, L. M. (2023). An imperative role of 6G communication with perspective of industry 4.0: Challenges and research directions. *Sustainable Energy Technologies and Assessments*, 56, 103047.
9. Jagannath, J., Ramezanpour, K., & Jagannath, A. (2022). Digital twin virtualization with machine learning for IoT and beyond 5G networks: Research directions for security and optimal control. In *Proceedings of the 2022 ACM Workshop on Wireless Security and Machine Learning* (pp. 81–86).
10. Han, H., Yao, J., Wu, Y., Dou, Y., & Fu, J. (2024). Quantum communication based cyber security analysis using artificial intelligence with IoMT. *Optical and Quantum Electronics*, 56(4), 565.
11. Consul, P., Budhiraja, I., Arora, R., Garg, S., Choi, B. J., & Hossain, M. S. (2024). Federated reinforcement learning based task offloading approach for MEC-assisted WBAN-enabled IoMT. *Alexandria Engineering Journal*, 86, 56–66.
12. Lakhan, A., Mohammed, M. A., Nedoma, J., Martinek, R., Tiwari, P., & Kumar, N. (2023). DRLBTS: Deep reinforcement learning-aware blockchain-based healthcare system. *Scientific Reports*, 13(1), 4124.
13. Haque, N. I., Rahman, M. A., & Uluagac, S. (2024). Formal threat analysis of machine learning-based control systems: A study on smart healthcare systems. *Computers & Security*, 139, 103709.
14. Mohammed, M. A., Lakhan, A., Zebari, D. A., Abd Ghani, M. K., Marhoon, H. A., Abdulkareem, K. H., & Martinek, R. (2024). Securing healthcare data in industrial cyber-physical systems using combining deep learning and blockchain technology. *Engineering Applications of Artificial Intelligence*, 129, 107612.
15. Patan, R., Ghantasala, G. P., Sekaran, R., Gupta, D., & Ramachandran, M. (2020). Smart healthcare and quality of service in IoT using grey filter convolutional based cyber physical system. *Sustainable Cities and Society*, 59, 102141.
16. Verma, R. (2022). Smart city healthcare cyber physical system: Characteristics, technologies and challenges. *Wireless personal communications*, 122(2), 1413–1433.
17. Olowononi, F. O., Rawat, D. B., & Liu, C. (2020). Resilient machine learning for networked cyber physical systems: A survey for machine learning security to securing machine learning for CPS. *IEEE Communications Surveys & Tutorials*, 23(1), 524–552.
18. Moin, A., Challenger, M., Badii, A., & Günnemann, S. (2022). A model-driven approach to machine learning and software modeling for the IoT: Generating full source code for smart Internet of Things (IoT) services and cyber-physical systems (CPS). *Software and Systems Modeling*, 21(3), 987–1014.
19. Chakraborty, C., Nagarajan, S. M., Devarajan, G. G., Ramana, T. V., & Mohanty, R. (2023). Intelligent AI-based healthcare cyber security system using multi-source transfer learning method. *ACM Transactions on Sensor Networks*. <https://doi.org/10.1145/3597210>
20. Rajawat, A. S., Bedi, P., Goyal, S. B., Shaw, R. N., & Ghosh, A. (2022). Reliability analysis in cyber-physical system using deep learning for smart cities industrial IoT network node. *AI and IoT for Smart City Applications*. https://doi.org/10.1007/978-981-16-7498-3_10
21. Suganyadevi, S., Priya, S. S., Menaha, R., Sathiya, S., & Jha, P. (2022). Smart healthcare in IoT using convolutional based cyber physical system. In *2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon)* (pp. 1–6). IEEE.
22. Priyadarshini, I., Sharma, R., Bhatt, D., & Al-Numay, M. (2023). Human activity recognition in cyber-physical systems using optimized machine learning techniques. *Cluster Computing*, 26(4), 2199–2215.
23. Razaque, A., Amsaad, F., Abdulgader, M., Alotaibi, B., Alsolami, F., Gulsezim, D., & Hariri, S. (2022). A mobility-aware human-centric cyber-physical system for efficient and secure smart healthcare. *IEEE Internet of Things Journal*, 9(22), 22434–22452.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.



Hemalatha Thanganadar Assistant Professor, Department of Health Informatics, College of Public Health and Tropical Medicine in Jazan University, Jazan, Saudi Arabia. She has nearly 20 years of teaching experience and 15 years of research experience. She has published nearly 20 research papers in International and National journals. She has presented many technical papers at National and International conferences. Her research area interests include Data Mining, the Internet of Things, Health Informatics, and Health Care.



Syed Mufassir Yaseen received the BCA and MCA degree from Kashmir University and Islamic University of Science and Technology, J&K, India in 2013 and 2017, respectively. He received the Ph.D. degree in Lovely Professional University Phagwara, India in 2021. From 2021, he has been Assistant Professor. His research interests include ML, mobile communication, ad hoc network, link layer and network layer protocol.



Dr. Shukla is holds a Ph.D. degree in Multi-core Architecture from Devi Ahilya Vishwavidyalaya Indore, and has received two gold medals for outstanding performance in my M.E. degree in Computer Engineering. Dr. Shukla's expertise lies in High Performance Computing, which he applies to various domains, such as BlockChain, Cloud Computing, and Artificial Intelligence. He has published more than 100 papers in reputed journals, and has developed and honed multiple skills, such as University Teaching, Research, and Patent. His goal is to advance the knowledge and innovation in Computer Engineering, and to inspire and empower the students and colleagues to achieve their academic and professional aspirations.



Ankur Singh Bist is currently working as Associate Professor at GEHU BHIMTAL. His area of research is Machine Learning and computer virology. He has written more than 200 research papers. He has worked as reviewer/editor in more than 400 conferences/journals. He is active member of various research societies and educational group. He has received 5 international awards and medals of honours by renowned societies. He has been honoured with various honorary titles/positions like Visiting Professor, Journal editor and mentors by various educational groups and NGOs.



Shavkatov Navruzбек Shavkatov received the BCA and MCA degree from Karshi Engineering Economics Institute and Tashkent Institute of Finance, Tashkent Uzbekistan in 2016 and 2018, respectively. He received the Ph.D. degree in Tashkent Institute of Finance, Uzbekistan in 2021. From 2021, he has been Assistant Professor. His research interests include IoT, mobile communication, data analysis.



P. Vijayakumar is completed his Ph.D. in Wireless Communication and Network Security at Pondicherry University, Pondicherry in 2015. He acted as a member in many professional bodies like ISTE, IET, CSI, and IAENG. He received a research award for his wonderful contribution to research from the Vellore Institute of Technology, Chennai. His area of specialization is AI with Cybersecurity, Hardware Security, Cryptographic Algorithms, ML/DL Algorithms, Blockchain technology Security, Security in Internet of Things, Cryptography, and 5G & 6G Network Securityes.

Authors and Affiliations

Hemalatha Thanganadar¹ · Syed Mufassir Yaseen² · Surendra Kumar Shukla³ · Ankur Singh Bist⁴ · Shavkatov Navruzbeq Shavkatovich⁵ · P. Vijayakumar⁶

✉ Hemalatha Thanganadar
hthanganadar@jazanu.edu.sa

- ¹ Department of Health Informatics, College of Public Health and Tropical Medicine, Jazan University, Jazan 45142, Kingdom of Saudi Arabia
- ² Department of Computer Science and Application, Dr. Vishwanath Karad MIT World Peace University, Pune, Mumbai, India
- ³ Department of Computer Engineering, SVKM'S NMIMS MPSTME Shirpur Campus, Dhule, Maharashtra, India
- ⁴ Graphic Era Hill University - Bhimtal Campus, Nagri Gaon, Uttarakhand, India
- ⁵ The Department of Corporate Finance and Securities, Tashkent State University of Economics, Tashkent, Uzbekistan
- ⁶ School of Electronic Engineering, Vellore Institute of Technology, Chennai, Tamilnadu, India