*Computers, Materials & Continua*
DOI: 10.32604/cmc.2022.025760
***Article***

Tech Science Press

# Deep Learning Enabled Disease Diagnosis for Secure Internet of Medical Things

**Sultan Ahmad[1], Shakir Khan[2], Mohamed Fahad AlAjmi[3], Ashit Kumar Dutta[4], L. Minh Dang[5], Gyanendra Prasad Joshi[6] and Hyeonjoon Moon[6,*]**

[1]Department of Computer Science, College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Alkharj, 11942, Saudi Arabia
[2]College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh, 11432, Saudi Arabia
[3]College of Pharmacy, King Saud University, Riyadh, 11451, Saudi Arabia
[4]Department of Computer Science and Information System, College of Applied Sciences, AlMaarefa University, Riyadh, 11597, Saudi Arabia
[5]Department of Information Technology, FPT University, Ho Chi Minh City, Vietnam
[6]Department of Computer Science and Engineering, Sejong University, Seoul, 05006, Korea
*Corresponding Author: Hyeonjoon Moon. Email: hmoon@sejong.ac.kr
Received: 03 December 2021; Accepted: 02 March 2022

**Abstract:** In recent times, Internet of Medical Things (IoMT) gained much attention in medical services and healthcare management domain. Since healthcare sector generates massive volumes of data like personal details, historical medical data, hospitalization records, and discharging records, IoMT devices too evolved with potentials to handle such high quantities of data. Privacy and security of the data, gathered by IoMT gadgets, are major issues while transmitting or saving it in cloud. The advancements made in Artificial Intelligence (AI) and encryption techniques find a way to handle massive quantities of medical data and achieve security. In this view, the current study presents a new Optimal Privacy Preserving and Deep Learning (DL)-based Disease Diagnosis (OPPDL-DD) in IoMT environment. Initially, the proposed model enables IoMT devices to collect patient data which is then preprocessed to optimize quality. In order to decrease the computational difficulty during diagnosis, Radix Tree structure is employed. In addition, ElGamal public key cryptosystem with Rat Swarm Optimizer (EIG-RSO) is applied to encrypt the data. Upon the transmission of encrypted data to cloud, respective decryption process occurs and the actual data gets reconstructed. Finally, a hybridized methodology combining Gated Recurrent Unit (GRU) with Convolution Neural Network (CNN) is exploited as a classification model to diagnose the disease. Extensive sets of simulations were conducted to highlight the performance of the proposed model on benchmark dataset. The experimental outcomes ensure that the proposed model is superior to existing methods under different measures.

**Keywords:** Internet of medical things; privacy; security; encryption; radix tree; deep learning

## 1 Introduction

Internet of Medical Things (IoMT) is an environment of clinical systems, healthcare devices, wearable devices, and interconnected sensors [1–3]. The concept ensures seamless functioning and inter-communication of numerous healthcare applications to increase the quality of medical treatment, provide timely medical replies and reduce costs incurred upon health care. It mainly encompasses the improvements made in sensor networks, mobile devices, Big Data Analysis (BDA), wireless communications, and Cloud Computing (CC) to achieve seamless communication of medical data. IoMT has transformed the healthcare industry radically by distributing personalized and targeted medication. The increased penetration of medical devices across global healthcare settings brought various advantages. However, it has also increased the privacy and security problems in multiple folds. The modern healthcare system gathers and processes complex and frequent life-critical medical data and makes crucial decisions depending on the data [4]. In this background, cybercriminals target vulnerable areas in IoMT devices. Though they cannot obtain significant access to the clinic network, they can gain illegal access to sensitive personal and healthcare data. Cyberattacks made on these healthcare and related devices tend to bring major physical and life-threatening injuries to the persons. Thus, privacy preserving method is considered to be one of the most important elements in this technology era.

IoMT utilizes different kinds of Machine Learning (ML) techniques to predict and understand healthcare modifications from separate standards [5,6]. Planned emotional support system can improve medical results (like decreased medicinal dishonesty) alike how hierarchical results increase (for example, efficiency development and homework) [7]. Additionally, ML methods can improve the framework for monitoring a person's day-to-day life activities by continuously learning from their personal data (for example, basic life signals) and help them achieve healthcare at a right time. This sort of data collection seems to be significant in improving the program without reservation and altering it during various phases. Once the data is gathered, it can be transferred to medical personnel or specialists to check the person's state [8]. To resolve the challenges faced in security, health care industry has found a method that utilizes Internet of Things (IoT). In this method, patients and healthcare professionals can communicate directly with each other through cell phone and a consultant can know the patient's conditions based on their specialization at clinic [9,10]. Furthermore, the patient need not regularly attend a tertiary hospital. The ultimate aim of this remote healthcare management is to stimulate patient healthcare and rapidly notify the healthcare professionals in case of an emergency [11].

The embedding of edge computation creates potential, powerful and delay-sensitive healthcare applications whereas CC provides the maximum assets for storage memory. In addition, edge and cloud computing bring efficient developments in healthcare field. In the application of modern computational methods, Deep Learning (DL) has been broadly utilized for understanding several domains such as object identification, Natural Language Processing, and image classification. Both compression and self-taught capability of DL helps in learning the features of input data automatically and hierarchically. This guarantees to emphasize the abnormal and hidden patterns in the data [12,13]. Consequently, DL method has evolved with much efficiency due to high number of IoT-based applications. A wide range of DL techniques has been utilized in problem solving methods with respect to healthcare. The usefulness of DL is achieved by utilizing deep layers which are in-built in the framework that makes the technique, a highly intensive one. Therefore, a minimum-powered edge device is not appropriate to improve the DL technique. Subsequently it cannot fulfill the highest computation cost necessities of DL approach too. The main challenge included in deploying effective

latency-aware health monitoring system is its dependency upon the embedding of DL implication to edge devices that have recovered computation capabilities.

The current research paper develops an Optimal Privacy Preserving and DL-based Disease Diagnosis (OPPDL-DD) method in IoMT environment. The proposed model primarily allows the IoMT devices to gather patient data and preprocess it to improve its quality. In order to reduce the computational complexity during diagnosis, Radix Tree structure is employed. The presented model also includes ElGamal public key cryptosystem with Rat Swarm Optimizer (EIG-RSO) to achieve security. At last, a hybridized HGRU-CNN model (comprising GRU and CNN models) is applied as a classification model for disease diagnosis. A wide-range of simulations was conducted to showcase the superiority of the proposed OPPDL-DD model upon benchmark dataset.

Rest of the paper is organized as follows. Section 2 discusses the works related to the domain, Section 3 briefs the proposed model, Section 4 validates the results, and Section 5 draws the conclusion for the study.

## 2 Literature Review

Cloud IoT has developed a skillful prediction and analytical method for diagnostics. Currently, several diagnostic methods are utilized to find out the diseases like breast cancer, brain disorders, Alzheimer's disease, cardiovascular diseases, thyroid diseases, hypotension, and leukemia heart disease [14]. For instance, a neuro-fuzzy framework is frequently utilized in creation systems, quality control, social security administrations, executive execution, and emergency situations. The medical services involve the facilitation of workers followed by maintenance and transit of medicinal assets. It also should meet the social security requirements of an individual. Zhang et al. [15] established a strong and Patented Privacy Data Protection system (PPDP). An individual's medical reports are encrypted in PPDP and then transmitted to cloud. For novel medical data, disease risk is determined based on the prediction pattern. Specifically, PPDP increases the application of arbitrary networks to examine the recent utilization of disease prediction methods, data encryption, and disease research.

Chen et al. [16] developed a predictive disease framework utilizing ML method for big data collected in healthcare network. This research was conducted with several prognostic methods that depend upon the information gathered from actual medical hospital located at Focal China between 2013 and 2015. To conquer the difficulty of fragmentary data, the method utilized inactive factor testing to retrieve the lost information. Additional modification was proposed in CNN to remove the probability of establishing unstructured multi-modal data, while utilizing medical diagnoses. Kaur et al. [17] conducted an extensive review of healthcare diagnostic procedures proposed so far. Big data techniques have been demonstrated to streamline the rapid growth of healthcare information. It initially checks the condition of big data in medical field though no crucial task has been performed in this domain. It is difficult to assume the influence of ML and big data in medical systems.

Lakshmanaprabu et al. [18] proposed a method to combat the confusions prevalent in the prognostics of diseases. To improve the prediction outcome, the study combined the concepts of fuzzy sets and instant case K. When Disease Prediction Support System (DPSS) assists in maintaining a significant data security, social security administration remains a major problem. DPSS was upgraded as Privacy Aware Disease Prediction Support System (PDPSS) by encrypting the homogeneous filler to secure personal sensitive data from illegal users. Din et al. [19] introduced IoT for ML in healthcare domain. ML is the most advanced technology these days which has gained the interests of several researchers and businesses and has experienced a rapid growth. The goal of ML technique is to

generate an inevitable connection with remote areas. In fact, ML of IoT depends upon self-sufficient networks that connect several gadgets with no human interaction.

Gupta et al. [20] proposed a common prediction model for heart disease in cloud computing. The previous challenges faced in medical diagnostics, especially, heart disease prediction can be resolved by ML and CC methods. The study determined a set of approaches to recommend a suitable method that can assist physicians in predicting heart disease based on the personal data of individuals. Liu et al. [21] presented a cloud healthcare system framework for Digital Twin Health (CloudDTH). The idea of Digital Twin Health (DTH) was deliberated and upgraded the DTH method. Amin et al. [22] proposed a significant data mining method that can enhance the prediction accuracy of Cardiovascular Diseases (CVD). These prediction methods are created by utilizing seven factors as alternate classification packages. Ali et al. [23] developed an IoT-based system for oncology domain. This system is utilized to efficiently test a person's physical conditions for displaying the thinness of apparent medicine and foods.

## 3 The Proposed Model

All the processes included in the proposed OPPDL-DD method are exhibited in Fig. 1. As per the figure, IoMT devices gather medical data, preprocess it, and effectively organize it with the help of Radix tree. Followed by, EIG-RSO algorithm is applied to encrypt the data for achieving privacy during data transmission and storage. Lastly, HGRU-CNN-based diagnostic process is executed to determine the presence of disease.

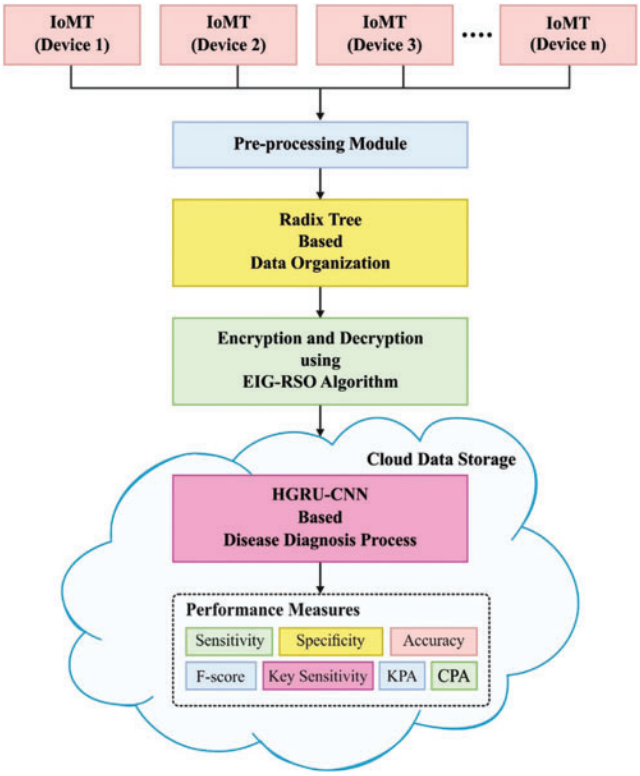


**Figure 1:** Working process of OPPDL-DD model

### *3.1 Radix Tree Structure*

Once the input medical data is gathered and preprocessed, radix tree is applied owing to its easier mechanism. It is a memory-oriented optimized trie in which every individual node has a child and is interconnected with two nodes. As a result, each interior node holds a minimum of two child nodes. On the contrary to traditional trie, the labeling of edges is done through succeeding and lonely characters. Fig. 2 illustrates the structure of Radix tree. It generates a compact set, particularly in case of long-sized strings. In radix tree, the height of the tree is mainly based on key length which does not defines the components that exist in the tree. It requires zero rebalancing function whereas every insertion order leads to an identical tree [24]. The keys are stored in a lexicographic pattern. The route, from the leaves, represents their keys. So, the keys are stored internally and can be decrypted from the routes. A pair of nodes is available in radix tree and are named after inner and leaf nodes. The inner node is represented by an array of 2 s pointers. Upon traversing, a $s$ bit part of the key can be used as an index to the array. Consequently, the subsequent child node can be identified without any extra comparison. The parameter $s$ can be named as the span utilized to analyze the outcomes of radix tree identified by tree height. The level count of intrinsic nodes, available to store $k-$ bit keys, are represented herewith.

$$\text{No. of levels} = \frac{\text{k}}{s} \tag{1}$$

The radix trie saves $k$ bit keys with $k/s$ levels of interior nodes.

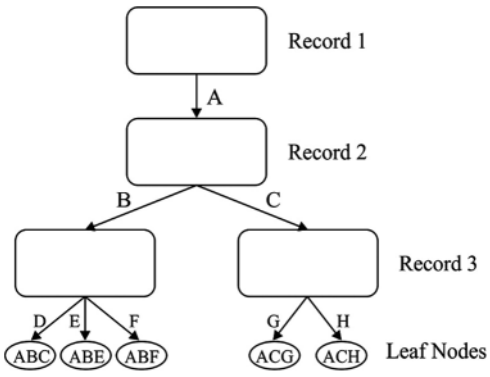


**Figure 2:** Structure of radix tree

### *3.2 Encryption Using EIG-RSO Algorithm*

At this stage, the healthcare information is encrypted utilizing EIG-RSO algorithm to safeguard the data during transmission and storage. The presented EIG technique is defined on the basis of discrete logarithmic problem which is complex for a finite field. It encompasses three processes such as key generation, encryption, and decryption. Primarily, the generation of keys plays a vital part in this cryptosystem as it affects the outcome of complete model. Besides, it is an asymmetric key encryption technique that makes use of Diffie-Hellman key exchange algorithm. It comprises of a private key $xi \in Zi^{*}_{qi'}$ with its corresponding public key being $yi \equiv (gi')^{xi} \bmod qi$. Here, $gi'$ denotes the generator for $Gi_1$ with prime order $qi'$. In this paper, EIG algorithm is optimized with the help of ROS algorithm during private key generation process. It resulted in the optimal generation of keys and a considerable increase in security.

Here, both encrypted data m$i \in Gi_1$ as well as public key $yi$ are described as a pair $ci_1 \equiv (\mathrm{g}i')^{\mathrm{n}}$ mod $qi$, $ci_2 \equiv yi^{ri}\mathrm{m}i$ mod $qi$, where $ri$ specifies a random number. Besides, the decrypted ciphertext $\{ci_1,\ ci_2\}$ and the private key $xi$ are defined by $\mathrm{mi} \equiv ci_2\left(ci_1^{xi}\right)^{-1}$ mod $qi$. Predominantly, this technique includes an identical ciphertext with selected-plaintext attacks for each probabilistic polynomial-time adversary, $Ai$. Alternatively, the data is encrypted randomly from two distinct messages, decided by $Ai$. The success potential of $Ai$, to recognize the selected message, gets trivially enhanced over arbitrary estimation. EIG technique is represented as a game concept with a $Ci$ challenger and an attacker, $Ai$.

- Originally, $Ai$ elects two dissimilar messages i.e., $\mathrm{m}i_0, \mathrm{m}i_1 \in Gi_1$ and forwards it to $Ci'$.
- Followed by, the technique determines $Ci'$ selecting $ai \in \{0, 1\}$ and $ri_1, xi \in Zi^*_{qi'}$ randomly and put $yi \equiv (\mathrm{g}i')^{xi}$ mod $qi$, $ci_1 \equiv (\mathrm{g}i')^{ri}$ mod $qi$ and $ci_2 \equiv (\mathrm{g}i')^{rixi}\ \mathrm{m}i_{ai}$ mod $qi$. Furthermore, $Ci'$ gives $Ai$ as $\mathrm{g}i'$, $yi$, $ci_1$, and $ci_2$.
- Determine the challenge as $Ci'$ and ask $Ai$ regarding $ai$.
- Find the guess as $Ai$ offering $ai'$ and forward it to return to $Ci'$.

For optimal private key generation, RSO algorithm is employed. Rats are medium-sized long-tail rodents that are classified based on its weight and size. It consists of two major classes such as brown and black rats. In rat's family, male rats are called 'bucks' while the female rats are called 'does'. They have a common behaviour in nature i.e., socially smart. It grooms itself and gets involved in various events like chasing, tumbling, boxing, and jumping. Rats are territorial animals and exist as a collection of females and males [25]. Rats are highly aggressive at most of the instances which result in the death of group members. This aggressive nature remains a major stimulation of this task when fighting and chasing the prey. In this study, both fighting and chasing nature of the rats are considered for mathematical models to implement RSO technique and execute optimization. This section defines the nature of rats in terms of fighting and chasing.

### *3.2.1 Chasing the Prey*

Commonly, rats are social animals that chase the prey in a set due to their social agonistic nature. To determine the mathematical nature of rats, optimum search agent is considered which has an understanding about the position of the prey. Another search agent can upgrade their location in line with the location accomplished by optimum searching agent. The subsequent formula expresses the condition.

$$\vec{P} = \mathrm{A} \cdot \vec{\mathrm{P}}_i(\mathrm{x}) + \mathrm{C} \cdot \left(\vec{\mathrm{P}}_r(\mathrm{x}) - \vec{\mathrm{P}}_i(\mathrm{x})\right) \tag{2}$$

While $\vec{\mathrm{P}}_i(\mathrm{x})$ represents the location of rat, $\vec{\mathrm{P}}_r(\mathrm{x})$ indicates the optimum solution. Both $A$ and $C$ variables are estimated herewith.

$$A = R - x \times \left(\frac{R}{\mathrm{Max}_{Iteration}}\right) \tag{3}$$

where, $x = 0, 1, 2, \cdots, \mathrm{Max}_{Iteration}$

$$C = 2 \cdot rand\ (\ ) \tag{4}$$

Thus, $R$ and $C$ denote the arbitrary values between [0, 2], and [1, 5] similarly. The variables such as $A$ and $C$ are accountable for high exploitation and exploration on iteration.

### *3.2.2 Fighting with Prey*

The mathematical fighting procedure of rats with prey can be defined as given herewith.

$$\vec{P}_i(x+1) = \left|\vec{P}_r(x) - \vec{P}\right| \tag{5}$$

In this equation, $\vec{P}_i(x+1)$ represents the upgraded location of the following rat. It stores the optimum solutions and upgrades the location of other searching agents regarding optimum search agents. The flowchart and the steps (Fig. 3) followed in RSO algorithm are given herewith.

1. Initiate rat population $P_i$ in which $i = 1, 2, \ldots, n$.
2. Choose the primary variables of RSO i.e., $A$, $C$, and $R$.
3. Estimate the fitness values of all searching agents.
4. Examine the optimum searching agent in the provided searching space.
5. Upgrade the positions of searching agent by utilizing Eq. (5).
6. Validate whether all the search agents exceed the boundaries of searching space after which modify it.
7. Again, estimate the upgraded searching agent fitness values and vector $P_r$, when there exists an optimum solution compared to prior optimum solution.
8. End the method after the ending conditions are fulfilled. Or else, proceed to Step 5.
9. Return the attained optimum and best solutions.

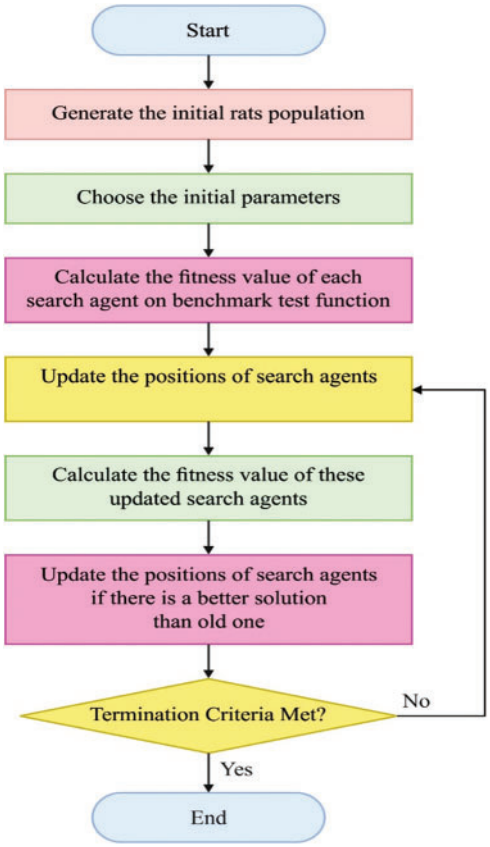


**Figure 3:** Flowchart of RSO algorithm

### *3.3 HGRU-CNN Based Disease Diagnosis Process*

During disease diagnosis process, HGRU-CNN model is implemented to determine the optimal class label of the employed medical data.

GRU is a variation of Long Short Term Memory (LSTM) with a gated RNN framework and comparative LSTM. It consists of two gates such as reset gate and update gate in GRU and three more gates such as input, output, and forgetting gates in LSTM; simultaneously, GRU have some trained variables compared to LSTM. Thus, GRU converges faster compared to LSTM in training. GRU framework is demonstrated in Fig. 4, where $\sigma$ and tanh denote the activation functions, $c^{\langle t-1\rangle}$ indicates the input of present unit which is also the output of prior unit, $c^{\langle t\rangle}$ represents the output of present unit and is related to the input of following unit. $x^{\langle t\rangle}$ represents the input of trained information, $\hat{y}$ indicates the unit results created by activation function, $\Gamma_r$ and $\Gamma_u$ denote update and reset gates, correspondingly, and the candidate activation $\tilde{c}^{\langle t\rangle}$ is calculated equally to conventional recurrent unit [26]. Here, GRU consists of two gates namely update gate that maintains prior data to the present state; the value of $\Gamma_u$ extents from zero to one, the nearer $\Gamma_u$ is to 0, the prior the data it is recollected. The second one is reset gate which is utilized to define either the present state or prior data is to be integrated. The value of $\Gamma_r$ extends from *Reject*1 to one, when the value of $\Gamma_r$ becomes smaller, then it ignores the prior data. Based on this scenario, GRU equation is given herewith.

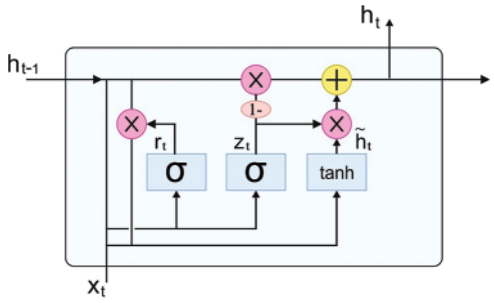


**Figure 4:** Structure of GRU

$$\begin{aligned}
\Gamma_u &= \sigma\left(\omega_u\left[c^{\langle t-1\rangle}, x^{\langle t\rangle}\right] + b_u\right),\\
\Gamma_r &= \sigma\left(\omega_r\left[c^{\langle t-1\rangle}, x^{\langle t\rangle}\right] + b_r\right)\\
\tilde{c}^{\langle t\rangle} &= tanh\left(\omega_c\ \left[\Gamma_r * c^{\langle t-1\rangle},\ x^{\langle t\rangle}\right] + b_c\right),\\
c^{\langle t\rangle} &= (1-\Gamma_u) * c^{\langle t-1\rangle} + \Gamma_u * \tilde{c}^{\langle t\rangle},
\end{aligned} \tag{6}$$

where $\omega_u$, $\omega_r$, and $\omega_c$ denote the trained weight matrices of reset and update gates, and candidate activation $\tilde{c}^{\langle t\rangle}$, correspondingly while $b_u$, $b_r$, and $b_c$ denote the bias vectors. CNN is a kind of Artificial Neural Network (ANN) that could operate under high dimension data. It is generally employed in video recognition, text categorization, and visual images. The spatiotemporal matrix for this CNN is given herewith.

$$X = \begin{bmatrix} X_1(1) & X_1(2) \cdots & X_1(\mathrm{n}) \\ X_2(1) & X_2(2) \cdots & X_2(\mathrm{n}) \\ \vdots & \vdots \quad \ddots & \vdots \\ X_{\mathrm{k}}(1) & X_{\mathrm{k}}(2) \cdots & X_{\mathrm{k}}(\mathrm{n}) \end{bmatrix} \tag{7}$$

where $k$ denotes the $k^{th}$ smart sensor, $n$ indicates the $n^{th}$ time sequence, and $X_k(n)$ denotes the data recorded by $k^{th}$ smart sensor on $n$ time. In order to extract the feature from spatiotemporal matrix and to process the spatiotemporal matrix, CNN is utilized.

In order to leverage the best out of GRU method such as operations of medical data and to reap the benefits of CNN method i.e., handling high dimension data, a hybrid GRU-CNN hybrid NN is used. The architecture of the presented GRU-CNN hybrid model comprises of both CNN and GRU modules [27]. The data gathered through IoMT devices acts as the input. CNN method utilizes shared weights and local connection to extract direct local features from medical data and attains efficient depiction by pooling and convolution layers. CNN framework comprises of flattening function and two convolution layers. All the convolution layers consist of pooling and convolution operations. Later, in secondary pooling function, high dimension data is flattened to 1D data, while the output of CNN method is related to Fully Connected (FC) layer. Alternatively, the goal of GRU method is to conquer long-term dependencies. This method can acquire beneficial data in historical information for a long time by memory cell and ineffective data is forgotten by the forget gate. The inputs of GRU method represent the input data; the method has several GRUs, and the outputs of each GRU are related to FC layer. Lastly, the disease diagnosis outcomes are attained by computing the mean values of entire neurons in FC layer.

## 4 Experimental Validation

Fig. 5 and Tab. 1 shows the results of comparative analysis between the proposed OPPDL-DD approach and existing techniques.

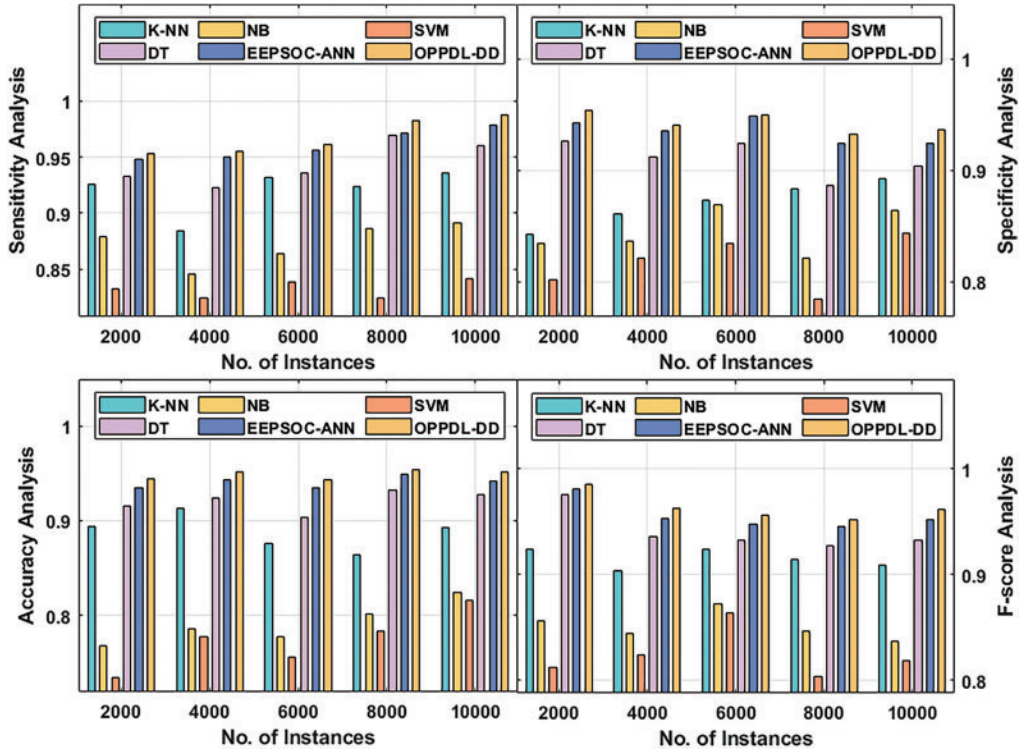


**Figure 5:** Results of the analysis of OPPDL-DD methodology under different measures

**Table 1:** Comparative analysis results of existing methods and the presented OPPDL-DD model

| Sensitivity | | | | | | |
|---|---|---|---|---|---|---|
| No. of instances | K-NN | NB | SVM | DT | EEPSOC-ANN | OPPDL-DD |
| 2000 | 0.926 | 0.879 | 0.832 | 0.933 | 0.948 | 0.953 |
| 4000 | 0.884 | 0.846 | 0.824 | 0.923 | 0.950 | 0.955 |
| 6000 | 0.932 | 0.864 | 0.839 | 0.936 | 0.956 | 0.961 |
| 8000 | 0.924 | 0.886 | 0.824 | 0.969 | 0.972 | 0.983 |
| 10000 | 0.936 | 0.891 | 0.842 | 0.960 | 0.979 | 0.988 |
| Specificity | | | | | | |
| No. of instances | K-NN | NB | SVM | DT | EEPSOC-ANN | OPPDL-DD |
| 2000 | 0.842 | 0.834 | 0.802 | 0.926 | 0.943 | 0.954 |
| 4000 | 0.861 | 0.836 | 0.821 | 0.912 | 0.935 | 0.941 |
| 6000 | 0.873 | 0.869 | 0.834 | 0.924 | 0.949 | 0.950 |
| 8000 | 0.883 | 0.821 | 0.784 | 0.886 | 0.924 | 0.932 |
| 10000 | 0.893 | 0.864 | 0.843 | 0.904 | 0.924 | 0.936 |
| Accuracy | | | | | | |
| No. of instances | K-NN | NB | SVM | DT | EEPSOC-ANN | OPPDL-DD |
| 2000 | 0.894 | 0.768 | 0.734 | 0.916 | 0.935 | 0.944 |
| 4000 | 0.913 | 0.786 | 0.777 | 0.924 | 0.943 | 0.951 |
| 6000 | 0.876 | 0.778 | 0.756 | 0.904 | 0.935 | 0.943 |
| 8000 | 0.864 | 0.801 | 0.784 | 0.932 | 0.949 | 0.954 |
| 10000 | 0.893 | 0.824 | 0.816 | 0.928 | 0.942 | 0.952 |
| F-score | | | | | | |
| No. of instances | K-NN | NB | SVM | DT | EEPSOC-ANN | OPPDL-DD |
| 2000 | 0.924 | 0.856 | 0.812 | 0.976 | 0.981 | 0.985 |
| 4000 | 0.903 | 0.844 | 0.824 | 0.936 | 0.953 | 0.963 |
| 6000 | 0.924 | 0.872 | 0.864 | 0.932 | 0.947 | 0.956 |
| 8000 | 0.914 | 0.846 | 0.804 | 0.927 | 0.945 | 0.952 |
| 10000 | 0.909 | 0.837 | 0.819 | 0.933 | 0.952 | 0.961 |

A sensitivity analysis was conducted for the proposed OPPDL-DD method and existing techniques in terms of number of instances. For instance, on the applied 2000 instances, OPPDL-DD model achieved a sensitivity of 0.953, whereas the k-nearest neighbor (K-NN), Naïve Bayes (NB), Support Vector Machine (SVM), Decision Tree (DT), and EEPSOC-ANN models obtained the sensitivity values such as 0.926, 0.879, 0.832, 0.933, and 0.948, respectively. Besides, on the applied 4000 instances, the proposed OPPDL-DD model attained a sensitivity of 0.955, whereas other models such as K-NN, NB, SVM, DT, and EEPSOC-ANN obtained the sensitivity values such as 0.884, 0.846, 0.824, 0.923, and 0.950, respectively. Also, on the applied 6000 instances, the presented OPPDL-DD technique obtained a sensitivity value of 0.932, whereas K-NN, NB, SVM, DT, and EEPSOC-ANN models reached 0.884, 0.864, 0.839, 0.936, and 0.956 sensitivity values correspondingly. Additionally, on the applied 8000 instances, the proposed OPPDL-DD system achieved a sensitivity of 0.983, whereas K-NN, NB, SVM, DT, and EEPSOC-ANN models obtained the following sensitivity values; 0.924, 0.886, 0.824, 0.969, and 0.972, respectively. Furthermore, on the applied 10000 instances, OPPDL-DD technique attained a sensitivity of 0.988, whereas other techniques such as K-NN, NB, SVM, DT, and EEPSOC-ANN obtained the following sensitivity values namely, 0.936, 0.891, 0.842, 0.960, and 0.979.

The authors conducted the specificity analysis for both the proposed OPPDL-DD method and the existing approaches in terms of number of instances. For instance, on the applied 2000 instances, the proposed OPPDL-DD approach achieved a specificity of 0.941, whereas K-NN, NB, SVM, DT, and EEPSOC-ANN models obtained the specificity values namely, 0.842, 0.834, 0.802, 0.926, and 0.943. Additionally, on the applied 6000 instances, OPPDL-DD system accomplished a specificity of 0.950, where K-NN, NB, SVM, DT, and EEPSOC-ANN techniques reached the specificity values namely, 0.873, 0.869, 0.834, 0.924, and 0.949, respectively. Likewise, on the applied 10000 instances, the proposed OPPDL-DD model obtained a specificity of 0.936, whereas K-NN, NB, SVM, DT, and EEPSOC-ANN models obtained the specificity values such as 0.893, 0.864, 0.843, 0.904, and 0.924 correspondingly.

Accuracy analysis was conducted for OPPDL-DD model and other existing methods in terms of number of instances. For example, on the applied 2000 samples, the proposed OPPDL-DD technology attained an accuracy of 0.944, whereas K-NN, NB, SVM, DT, and EEPSOC-ANN approaches reached the accuracy values such as 0.894, 0.768, 0.734, 0.916, and 0.935, respectively. Similarly, on the applied 6000 instances, OPPDL-DD model reached an accuracy of 0.943, whereas other approaches such as K-NN, NB, SVM, DT, and EEPSOC-ANN obtained the following accuracy values like 0.876, 0.778, 0.756, 0.904, and 0.935 correspondingly. Likewise, on the applied 10000 instances, OPPDL-DD system accomplished an accuracy of 0.952, while K-NN, NB, SVM, DT, and EEPSOC-ANN methodologies obtained the accuracy values such as 0.893, 0.824, 0.816, 0.928, and 0.942, respectively.

F-score analysis was conducted for OPPDL-DD against current approaches under different number of instances. For instance, on the employed 2000 instances, the proposed OPPDL-DD methodology attained an F-score of 0.985, whereas K-NN, NB, SVM, DT, and EEPSOC-ANN techniques obtained the following F-scores such as 0.924, 0.856, 0.812, 0.976, and 0.981, respectively. At last, on the applied 6000 instances, the presented OPPDL-DD approach obtained an F-score of 0.956, whereas K-NN, NB, SVM, DT, and EEPSOC-ANN methods attained the F-scores such as 0.924, 0.872, 0.864, 0.932, and 0.947, respectively. Followed by, on the applied 10000 instances, OPPDL-DD technique achieved an F-score value of 0.961, whereas other approaches such as K-NN, NB, SVM, DT, and EEPSOC-ANN reached F-scores namely, 0.909, 0.837, 0.819, 0.933, and 0.952.

Tab. 2 and Fig. 6 shows the key sens. analysis results accomplished by EIG-RSO algorithm and existing techniques. From the figure, it can be stated that EIG-RSO algorithm accomplished the optimal results for key sens. analysis. For instance, under the presence of 10%, EIG-RSO algorithm achieved an effective key sensitivity of 0.016, where Genetic Algorithm (GA) method, CM-LA model, Lion Algorithm (LA) process, Cuckoo Search (CS) algorithm, Firefly (FF) system, and Particle Swarm Optimization (PSO) techniques achieved poor key sens. values namely, 0.053, 0.038, 0.256, 0.041, 0.038, and 0.017. Moreover, under the presence of 20%, EIG-RSO model demonstrated an effective key sens. of 0.010, while other methods such as GA, CM-LA, LA, CS algorithm, FF and PSO accomplished poor key sens. values such as 0.051, 0.041, 0.270, 0.068, 0.026, and 0.011, correspondingly. Furthermore, under the presence of 40%, EIG-RSO methodology depicted an effective key sens. of −0.030, while GA method, CM-LA model, LA process, CS algorithm, FF system, and PSO techniques achieved poor key sens. values such as 0.043, −0.017, 0.173, 0.176, 0.012, and 0.009, respectively. Besides, under the presence of 60%, the EIG-RSO technique exhibited an effective key sens. of 0.009, while GA method, CM-LA approach, LA, CS process, FF model, and PSO techniques achieved poor key sens. values namely, 0.017, 0.010, 0.124, 0.156, 0.097, and 0.018, respectively. Additionally, under the presence of 80%, EIG-RSO approach outperformed other methods and achieved an effective key sens. of −0.045, while GA method, CM-LA model, LA process, CS algorithm, FF system, and PSO techniques accomplished poor key sens. values namely, 0.068, −0.036, 0.074, 0.232, 0.017, and 0.077.

**Table 2:** Key sensitivity analysis results with developed EIG-RSO models

| (%) | Key sensitivity analysis | | | | | | |
|---|---|---|---|---|---|---|---|
| | EIG-RSO | CM-LA | LA | CS | FF | PSO | GA |
| 10 | 0.016 | 0.038 | 0.256 | 0.041 | 0.038 | 0.017 | 0.053 |
| 20 | 0.010 | 0.041 | 0.270 | 0.068 | 0.026 | 0.011 | 0.051 |
| 40 | −0.030 | −0.017 | 0.173 | 0.176 | 0.012 | 0.009 | 0.043 |
| 60 | 0.009 | 0.010 | 0.124 | 0.156 | 0.097 | 0.018 | 0.017 |
| 80 | −0.045 | −0.036 | 0.074 | 0.232 | 0.017 | 0.077 | 0.068 |
| 100 | −0.008 | −0.004 | 0.061 | 0.232 | 0.052 | 0.043 | 0.071 |

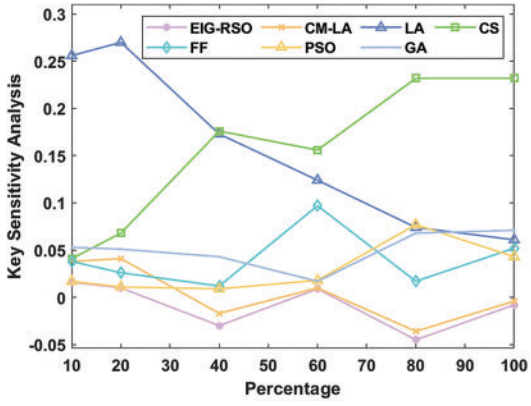


**Figure 6:** Key sensitivity analysis results of EIG-RSO models

Lastly, under the presence of 100%, EIG-RSO algorithm portrayed an effective key sensitivity of −0.008, whereas GA, CM-LA, LA, CS, FF, and PSO systems exhibited poor key sensitivity values namely, 0.071, −0.004, 0.061, 0.232, 0.052, and 0.043.

Figs. 7 and 8 depict the results from KPA and CPA analysis achieved by EIG-RSO algorithm against existing techniques. From the attained outcomes, it is apparent that EIG-RSO algorithm obtained KPA and CPA values such as −0.09868 and −0.04994 respectively. Simultaneously, PSO system gained inferior KPA and CPA results such as 0.091679 and 0.089142, respectively. Besides, other methodologies namely FF, CS, LA, GA, and CM-LA models too exhibited moderate results. From the abovementioned analysis and discussion, it is apparent that the developed model achieved excellent privacy and produced an effective disease diagnosis outcome.

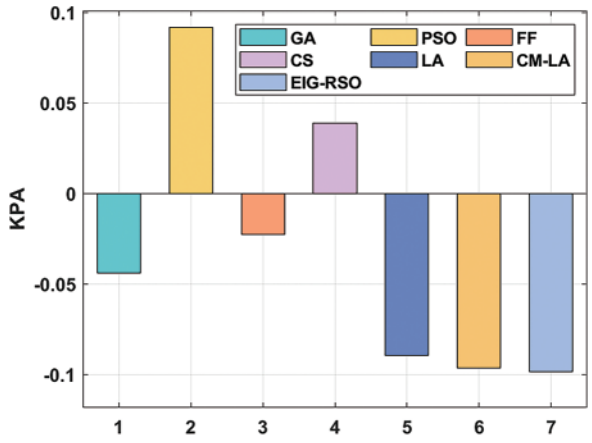


**Figure 7:** KPA analysis results of EIG-RSO approach with recent methodologies

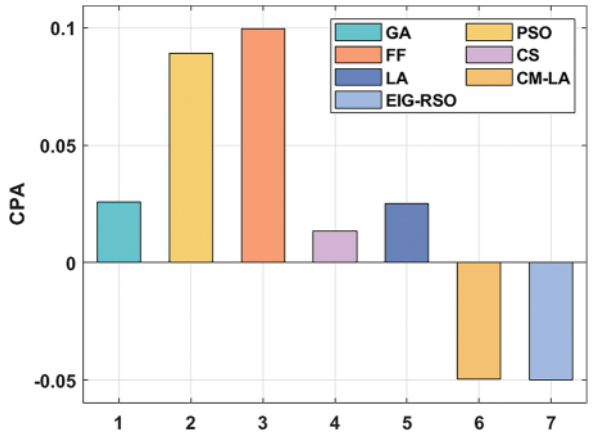


**Figure 8:** CPA analysis of EIG-RSO with recent methodologies

## 5 Conclusion

The current research paper has presented an effective OPPDL-DD method for privacy preserving and disease diagnosis in IoMT environment. Primarily, IoMT devices gather medical data which is effectively organized with the help of Radix tree. The application of Radix Tree helps in reducing the

computational complexity during diagnosis. Followed by, EIG-RSO algorithm is applied to encrypt the data and achieve privacy during data transmission and storage. Lastly, HGRU-CNN based diagnostic process is executed to determine the existence of disease. The results from a comprehensive experimental investigation proved the superiority of the proposed OPPDL-DD model on benchmark dataset. The stimulation outcome establishes that the proposed methodology is superior to existing models under various measures. In future, the developed OPPDL-DD models can be extended for real time hardware implementation.

**Funding Statement:** This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2020R1A6A1A03038540) and National Research Foundation of Korea (NRF) grant funded by the Korea government, Ministry of Science and ICT (MSIT) (2021R1F1A1046339) and by a grant (20212020900150) from "Development and Demonstration of Technology for Customers Bigdata-based Energy Management in the Field of Heat Supply Chain" funded by Ministry of Trade, Industry and Energy of Korean government.

**Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.

## References

[1] M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, I. Essop *et al.* "A survey on security threats and countermeasures in internet of medical things (IoMT)," *Transactions on Emerging Telecommunications Technologies*, 2020, https://doi.org/10.1002/ett.4049. Early View.

[2] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou *et al.* "Review of security and privacy for the internet of medical things (IoMT)," in 2019 in *15th Int. Conf. on Distributed Computing in Sensor Systems (DCOSS)*, Santorini Island, Greece, pp. 457–464, 2019.

[3] Y. Sun, F. P. W. Lo and B. Lo, "Security and privacy for the internet of medical things enabled healthcare systems: A survey," *IEEE Access*, vol. 7, pp. 183339–183355, 2019.

[4] F. A. Turjman, M. H. Nawaz and U. D. Ulusar, "Intelligence in the internet of medical things era: A systematic review of current and future trends," *Computer Communications*, vol. 150, pp. 644–660, 2020.

[5] K. C. Suneetha, R. S. Shalini, V. K. Vadladi and M. Mounica, "Disease prediction and diagnosis system in cloud based IoT: A review on deep learning techniques," *Materials Today: Proceedings*, 2020, https://doi.org/10.1016/j.matpr.2020.09.519. In Press.

[6] J. Uthayakumar, N. Metawa, K. Shankar and S. K. Lakshmanaprabu, "Intelligent hybrid model for financial crisis prediction using machine learning techniques," *Information Systems and e-Business Management*, vol. 18, no. 4, pp. 617–645, 2020.

[7] M. Hossain, S. M. R. Islam, F. Ali, K. S. Kwak and R. Hasan, "An internet of things-based health prescription assistant and its security system design," *Future Generation Computer Systems*, vol. 82, pp. 422–439, 2018.

[8] J. L. Hou and K. H. Yeh, "Novel authentication schemes for iot based healthcare systems," *International Journal of Distributed Sensor Networks*, vol. 11, no. 11, pp. 183659, 2015.

[9] P. Koti, P. Dhavachelvan, T. Kalaipriyan, S. Arjunan, J. Uthayakumar *et al.* "Heart disease prediction using hybrid harmony search algorithm with levi distribution," *International Journal of Mechanical Engineering and Technology*, vol. 9, no. 1, pp. 980–994, 2018.

[10] J. A. Alzubi, J. Selvakumar, O. A. Alzubi and R. Manikandan, "Decentralized internet of things," *Indian Journal of Public Health Research & Development*, vol. 10, no. 2, pp. 251, 2019.

[11] S. Sharma, K. Chen and A. Sheth, "Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems," *IEEE Internet Computing*, vol. 22, no. 2, pp. 42–51, 2018.

[12] S. Pothula, J. Uthayakumar, P. Koti, D. Poonurangam, S. Arjunan *et al.* "An efficient healthcare framework for kidney disease using hybrid harmony search algorithm," *Electronic Government, an International Journal*, vol. 16, no. 1, pp. 1, 2020.
[13] A. Khamparia, D. Gupta, V. H. C. de Albuquerque, A. K. Sangaiah and R. H. Jhaveri, "Internet of health things-driven deep learning system for detection and classification of cervical cells using transfer learning," *the Journal of Supercomputing*, vol. 76, no. 11, pp. 8590–8608, 2020.
[14] J. A. Alzubi, R. Manikandan, O. A. Alzubi, N. Gayathri and R. Patan, "A survey of specific IoT applications," *International Journal on Emerging Technologies*, vol. 10, no. 7, pp. 47–53, 2019.
[15] C. Zhang, L. Zhu, C. Xu and R. Lu, "PPDP: An efficient and privacy-preserving disease prediction scheme in cloud-based e-healthcare system," *Future Generation Computer Systems*, vol. 79, pp. 16–25, 2018.
[16] M. Chen, Y. Hao, K. Hwang, L. Wang and L. Wang, "Disease prediction by machine learning over big data from healthcare communities," *IEEE Access*, vol. 5, pp. 8869–8879, 2017.
[17] P. Kaur, M. Sharma and M. Mittal, "Big data and machine learning based secure healthcare framework," *Procedia Computer Science*, vol. 132, pp. 1049–1059, 2018.
[18] S. K. Lakshmanaprabu, S. N. Mohanty, S. S. Rani, S. Krishnamoorthy, J. Uthayakumar *et al.* "Online clinical decision support system using optimal deep neural networks," *Applied Soft Computing*, vol. 81, pp. 105487, 2019.
[19] I. U. Din, M. Guizani, J. J. P. C. Rodrigues, S. Hassan and V. V. Korotaev, "Machine learning in the internet of things: Designed techniques for smart cities," *Future Generation Computer Systems*, vol. 100, pp. 826–843, 2019.
[20] N. Gupta, N. Ahuja, S. Malhotra, A. Bala and G. Kaur, "Intelligent heart disease prediction in cloud environment through ensembling," *Expert Systems*, vol. 34, no. 3, pp. e12207, 2017.
[21] Y. Liu, L. Zhang, Y. Yang, L. Zhou, L. Ren *et al.* "A novel cloud-based framework for the elderly healthcare services using digital twin," *IEEE Access*, vol. 7, pp. 49088–49101, 2019.
[22] M. S. Amin, Y. K. Chiam and K. D. Varathan, "Identification of significant features and data mining techniques in predicting heart disease," *Telematics and Informatics*, vol. 36, pp. 82–93, 2019.
[23] F. Ali, S. M. R. Islam, D. Kwak, P. Khan, N. Ullah *et al.* "Type-2 fuzzy ontology–aided recommendation systems for IoT–based healthcare," *Computer Communications*, vol. 119, pp. 138–155, 2018.
[24] N. Krishnaraj, M. Elhoseny, E. L. Lydia, K. Shankar and O. ALDabbas, "An efficient radix trie -based semantic visual indexing model for large-scale image retrieval in cloud environment," *Software: Practice and Experience*, vol. 51, no. 3, pp. 489–502, 2021.
[25] G. Dhiman, M. Garg, A. Nagar, V. Kumar and M. Dehghani, "A novel algorithm for global optimization: Rat swarm optimizer," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 8, pp. 8457–8482, 2021.
[26] L. Wu, C. Kong, X. Hao and W. Chen, "A Short-term load forecasting method based on GRU-CNN hybrid neural network model," *Mathematical Problems in Engineering*, vol. 2020, pp. 1–10, 2020.
[27] L. Luo, "Network text sentiment analysis method combining LDA text representation and GRU-CNN," *Personal and Ubiquitous Computing*, vol. 23, no. 3–4, pp. 405–412, 2019.