HCIS | Human-centric Computing and Information Sciences

RESEARCH (Research Manuscript) **Open Access**

Human-centric Computing and Information Sciences (2023) 13:19
DOI: https://doi.org/10.22967/HCIS.2023.13.019
Received: May 7, 2022; Accepted: July 30, 2022; Published: April 30, 2023

IoT Integrated Edge Platform for Secure Industrial Application with Deep Learning

Saravana Balaji B[1,*], Wiesław Paja[2], Milos Antonijevic[3], Catalin Stoean[4], Nebojsa Bacanin[3], and Miodrag Zivkovic[3]

Abstract

Smart cities are composed of intelligent industrial things that enhance people's lives and save lives. Intelligent remote patient monitoring helps predict the patient's condition. Internet of Things (IoT), artificial intelligence (AI), and cloud computing have improved the healthcare industry. Edge computing speeds up patient data transmission and ensures latency, reliability, and response time. Nonetheless, the transmission of massive amounts of patient data may lead to IoT data security vulnerabilities, which is both a concern and a challenge. This research proposed a secure, scalable, and responsive patient monitoring system. This model used the lightweight attribute-based encryption (LABE), which encrypts and decrypts IoT patient data to protect cloud-based IoT patient data. Edge servers are positioned between the IoT and cloud to increase QoS and diagnose patient impairment. The deep belief network (DBN) predicts and monitors patient health. The bat optimization algorithm (BOA) optimizes the hyperparameters. This study used deep belief to identify hyper parameters and BOA for optimization. Swarm intelligence improves the prediction results and edge–cloud reaction time. The simulation environment assessed the secure patient health monitoring system to ensure its efficiency, security, and efficacy. The proposed model offers effective patient remote health monitoring through a secure edge–cloud–IoT environment with improved accuracy (97.9%), precision (95.6%), recall (94.6%), F1-score (94.9%), and FDR (0.06).

Keywords

Cloud Computing, Edge Computing, Internet of Things (IoT), Patient Health Monitoring, Smart Cities, Cryptography, Bat Algorithm, Deep Belief Network

1. Introduction

Internet of Things (IoT) uses medical sensors to sense patient data and interpret, and process, and respond to them in a timely manner over the network. Data from the sensing devices are transformed into natural scenarios, producing a smart environment. The innovation of IoT creates a smart environment that integrates the smart devices in the network to share, communicate, and perform a particular process. The smart modules in the network can perform these tasks with coordination between them. Smart cities

***Corresponding Author:** Saravana Balaji B (saravanabalaji.b@gmail.com)
[1]Department of Information Technology, Lebanese French University, Erbil, Iraq
[2]Institute of Computer Science, University of Rzeszów, Rzeszów, Poland
[3]Department for Informatics and Computing, Singidunum University, Belgrade, Serbia
[4]Department of Computer Science, University of Craiova, Craiova, Romania

include various applications such as healthcare, smart electricity, transportation, management, smart buildings, and sewerages. Through smart services, the smart data element is generated and used for smart city applications [1–5]. Cloud and edge computing provide the best services to smart cities due to the characteristics of smart node collaboration. Since the smart devices are located far away from the cloud server, edge computing is introduced to reduce the network traffic of the transmission, which in turn may lead to increased response time and traffic. Due to various reasons such as smart devices cooperation, 5G/6G network exploitation, and base station service providers, edge computing is also incorporated.

In smart cities, the real environment is changed into an automation environment based on the smart devices that provide reliable management of the data. It has various components including weather monitoring, smart homes, waste management, energy management, buildings, medical services, sewerage, air pollution control, monitoring of forest fire, traffic control, health monitoring, radiation level monitoring, intelligent shopping, smart maps, smart lighting, and vehicle auto diagnosis [1–3]. The integration of IoT–edge and cloud requires the healthcare system to be available everywhere to secure fast response for the patients and doctors. On the other hand, accessing medical hospitals is still a challenging issue in smart healthcare using smart devices. Patients with serious vital signs need instant solutions in the fastest way. Thus, the analyzed results must be accurate based on the previous analysis, and the response time should be minimized with reduced network latency. Therefore, smart healthcare is integrated with an edge–cloud environment to overcome the issues with the utilization of available resources and technologies in the smart city environment.

The revolution of smart devices in healthcare systems serves various significant purposes such as measuring the patient's blood sugar, body temperature, weight, blood pressure, and stress through wearable devices. Thus, the integration of edge–cloud–IoT is of utmost importance, both with regard to the real world and research. The smart remote patient healthcare monitoring system in the cloud IoT scenario consists of various kinds of patient biological data that are transmitted over the network and stored in the cloud anywhere [1]. Through the IoT network, the transmitted patient data gives rise to confidentiality and security issues that have to be addressed carefully [2]. Therefore, lightweight cryptography approaches are applied to provide security of the medical data that is necessary for the secure and safe management of patient medical information [3, 4].

Akhbarifar et al. [5] developed a remote health monitoring method using the lightweight block encryption approach to provide security of the patient data and applied various machine learning algorithms for the prediction of patient heart diseases. They concluded that the R-star approach performs better with accuracy of 95% than support vector machine (SVM), random forest (RF), J48, and multilayer perceptron (MLP). Jayaram and Prabakaran [6] proposed remote patient monitoring and rehabilitation with a privacy-preserving secure healthcare system using edge-level privacy-preserving additive homomorphic encryption. With the implementation of filtering and offloading decisions, this work reduces the network traffic and response time. The proposed adaptive weighted probabilistic classifier performs better with accuracy of 96.9% compared to other classifiers such as neural network, linear SVM, polynomial SVM, radial basis SVM, and sigmoid SVM. With this motivation, this paper proposes a secure edge–cloud–IoT-based smart city healthcare system to provide optimal on-time care to the patients. This proposed approach also ensures reduced latency and response time. The contributions of this work are as follows:

- Patients' sensitive health-related data are collected through IoT sensors using the wearable devices of the patients.
- Patients' sensitive data are encrypted using the lightweight attribute-based encryption (LABE) approach in the edge network to ensure the security and confidentiality of the patient medical data.
- The encrypted sensitive data are decrypted by the cloud processor for prediction. The decrypted data are preprocessed using normalization and scaling approaches to make the data balanced.
- The preprocessed data are used for the prediction process using the deep belief network (DBN) optimized with the bat optimization algorithm (BOA).

The predicted health status of the patient is monitored and notified to the healthcare providers in case of an emergency. The proposed edge–cloud–IoT-based healthcare monitoring was simulated and compared with existing models to prove the efficiency and security of the proposed system. The implementation of an edge network is expected to reduce the network latency and response time, with the implementation of optimization algorithms increasing the prediction accuracy of the classifiers.

The rest of this paper is organized as follows: Section 2 discusses the related work of smart patient health monitoring systems; Section 3 proposes a security method and a classification method for monitoring and diagnosing the patient's health status; Section 4 presents the simulated and obtained results with appropriate comparison; Section 5 presents the conclusion and provides ideas for future research directions.

2. Related Work

This section discusses the most relevant existing research works related to edge–cloud–IoT-based smart healthcare systems. Alrazgan [7] developed an edge–cloud-based healthcare system for smart cities, studying the offloading approaches for mobile edge computing using PSO, ACO, and DPSO to improve the quality of service of the network and concluding that DPSO performs better in terms of reducing latency and energy. Suryandari et al. [8] developed a remote patient monitoring system to manage the resources of the hospital effectively using patient monitoring at home through IoT. The systems provide data access and monitoring through the user-friendly gateway.

Liu et al. [9] developed a cloud-based system using a digital twin healthcare system to observe, analyze, and predict the elderly's health status through wearable medical devices for monitoring patients' health status and suggested innovations in the digital twin healthcare system. Ganesan and Sivakumar [10] and Nguyen et al. [11] developed a deep learning approach based on heart disease prediction in an IoT environment. Abdelaziz et al. [12] proposed a cloud–IoT-based medical monitoring system and analyzed various classification methods for the prediction of diabetes mellitus, hypertension, renal disorder, and heart disease. A lightweight selective encryption algorithm was proposed by Qui et al. [13] using a machine learning method to protect data security. Zhou et al. [14] developed a Fibonacci Q matrix-based logarithmic encryption for cyber systems. This method has been extended with fuzzy and guaranteed data security in a model proposed by Ma et al. [15]. Sun [16] studied cyber security approaches such as multi-authority-based encryption, key policy attribute-based encryption, fine-grain, trust, revocation, multi-tenant, trace approach, and hierarchical and proxy re-encryption to ensure security in the cloud. Abd El-Latif et al. [17] proposed a quantum walk-based encryption method with permutation phases in healthcare systems to protect patient data confidentiality without compromising the image encryption efficiency and robustness. Hassan et al. [18] developed a certificate-less public key encryption approach to protecting the authorized cloud server with an equality test scheme for smart healthcare systems. Hameed et al. [19] proposed a cipher blockchain advanced encryption model with Huffman coding and wavelet transform to improve data safety and efficiency of data storage between the stakeholders.

Ben Dhaou et al. [20] reviewed various wearable device techniques, algorithms, and technologies in terms of the Internet of medical things. They also surveyed the transformation methods used for fog computing with IoT devices. Cao et al. [21] proposed a medical health monitoring system with IoT and cloud computing using three terminals: sensor, gateway, and service. Based on the community and region, patients are efficiently monitored through GSM and the website. Zhang et al. [22] proposed the real-time health monitoring of patients through 5G mobile edge computing with IoT using an artificial intelligence algorithm for diagnosis. Table 1 compares the healthcare systems based on their merits and demerits [8, 23–28].

Security poses a major challenge in the medical industry. Medical data have to be personalized by hospital. There are many deep learning techniques using wireless sensor network (WSN) to improve the performance of IoT. Convolution neural network (CNN) for malware classification [29] and cognitive architecture for cyber security [30] require more time to identify the intrusions. Likewise, some research

[31–35] studies used machine learning-based feature extraction and classification for malware prediction. Bio-inspired robots are used with Internet of Medical Things (IoMT) for securing the data in cloud [36]. Blockchain-assisted cloud network for the security system [37] in cloud is implemented with less cost.

Table 1. Comparison of existing healthcare systems

Study	Method	Disadvantage	Advantage
Adebiyi et al. [23]	Optimized genetic algorithm-based feature selection is performed on the Gambia dataset using SVM kernel approaches	Model is complicated	Improved classification accuracy
Suryandari et al. [8]	Remote patient monitoring with efficient management of hospital resources	Lack of accuracy in disease diagnosis and high error in classification	Improved classification speed and outlier removal in IoT
Gupta et al. [24]	IoT-based remote patient monitoring system	The model is complicated, with increased computation time	Improved classification accuracy
Tan and Halim [25]	IoT-based healthcare monitoring and diagnosis system	A complicated model with maximum error and reduced computational speed	Optimal classification accuracy
Hiriyannaiah et al. [26]	LSTM-based patient health monitoring system	Increased computational speed	Improved classification accuracy
Arowolo et al. [27]	Optimized genetic algorithm with PCA and ICA for patient disease diagnosis and monitoring in IoT	Model is complicated	Optimal accuracy in classification
Vahidi Farashah et al. [28]	Clustering and deep learning-based patient disease analysis	Increased computation time	Improved classification accuracy

3. Proposed Methodology

The proposed patient health monitoring system integrates the cloud platform with an edge network to reduce latency, cost, and traffic. This section discusses the system model, encryption-decryption method, and disease prediction approaches.

3.1 System Model

The proposed secure edge–cloud–IoT-based patient remote health monitoring system is shown in Fig 1, which consists of four components: IoT network, edge network, cloud platform, and healthcare providers. The patient's medical data such as heart rate, body temperature, blood pressure, blood sugar, stress level, pulse counter, consciousness level, etc., are collected from IoT devices. The collected sensitive medical data are shared to the edge network through gateways. This edge network also provides computing and storage capability that is integrated with the cloud computing platform. Such collected data are processed in the edge layer to ensure security using a LABE algorithm that will protect the patient data from attackers. The encrypted data are sent to the cloud server through the cloud gateway. Next, the cloud platform is responsible for secure data processing, and it also provides central storage for the healthcare system. All the virtual machines in the cloud–edge platform ensure data security and integrity before processing. The cloud layer decrypts the sensitive medical data and preprocesses the information using normalization approaches to make the data balanced for improved prediction accuracy. The cloud layer then employs a deep learning model called DBN for the prediction of patients' vulnerabilities. The hyperparameters of the neural network are optimized using the BOA approach to avoid overfitting issues. Additionally, the optimization algorithm reduces the load of an edge–cloud environment with its heuristic searching behavior. Next, the healthcare providers can analyze the predicted data severity through

continuous monitoring and assessments. Based on the observed reports, the medical professionals are updated on the patient health status. In case of any vulnerabilities in inpatient health conditions, the emergency alert is given to doctors and patients' caretakers, with doctors providing online prescriptions remotely.

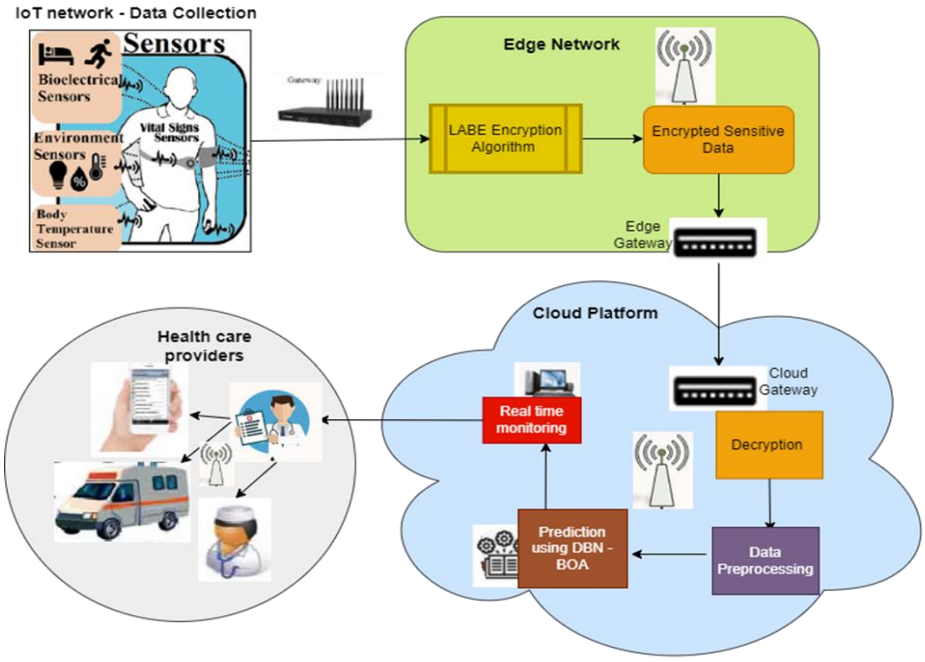

Fig. 1. Proposed secure edge–cloud–IoT-based remote patient health monitoring system.

3.2 IoT Network

This component is responsible for collecting the medical data of the patients through the IoT sensors and resources. The gathered patient medical data include blood cholesterol, heart rate, blood pressure, and other parameters sensed from the sensors attached to the patient's body or clothes through the body area network. Compared to other network devices, the body sensors are more vulnerable to attacks; thus, security is a major concern in transmitting patients' sensitive data over the network. Prior to being uploaded to the cloud server, the collected data are protected using a lightweight CP-ABE algorithm in the edge server, which will reduce the overhead of the cloud server. The IoT device data include the patient identification data and previous clinical data entered by the patient. The IoT device data for patient identification and previous clinical and present medical data are presented in Table 2. The following are the steps involved in the data collection process:

- IoT device data such as patient identification data and patients' previous medical data are entered.
- Patients' current medical data are collected from medical sensors.
- The collected medical data are sent to the next component for the encryption process.

3.3 Edge Network

This component is responsible for transferring the medical data to cloud storage with security measures. This will ensure data secrecy in the cloud in the distributed data storage. The security of the data is a major concern in the medical field since the patient's sensitive information are involved. Thus, patient data are encrypted before storing them in the edge and cloud server as follows:

- Read the collected medical data presented in Section 3.2.

- Encrypt the data using LABE and send the encrypted data to the cloud storage.

Table 2. Patient data collection in an IoT environment

Patient identification data	Patients' previous clinical data	Patient medical data gathered from sensors
Patient's national id	Height and weight	Oxygen saturation
Name	Smoker/alcohol drinker/drug user	Body temperature
Gender	Blood sugar	Blood pressure
Occupation	Hypertension history	Blood sugar
Mobile number	Blood cholesterol	Heart rate
Address	Blood pressure	Isolated systolic and diastolic blood pressure
		HDL (high-density lipoprotein) and LDL (low-density lipoprotein) cholesterol
		Respiratory rate

3.3.1 Lightweight attribute-based encryption (LABE) algorithm

The public key cryptography approach called attribute-based encryption provides secure access control of the medical data among the users. The access policy is based on the ciphertext and generated private key for the attributes. To decrypt the encrypted data (ciphertext), the user should have the private key of the attributes that satisfy the access policy. This approach consists of four processes: setup, key generation, encryption, and decryption. The algorithm steps are as follows:

Step 1 (Setup): This approach uses security parameter ρ to generate public key (P_k) in Equation (1) and master secret key (M_k) listed in Equation (2).

$$P_k = D_0, g, h = g^{\gamma}, f = g^{\frac{1}{\gamma}}, e(g,g)^{\delta} \tag{1}$$

$$M_k = \gamma, g^{\delta} \tag{2}$$

where γ, δ are random exponents ($\gamma, \delta \in Z_p$) and D_0 is bilinear prime order group p with generator g.

Step 2 (Key generation): The key generation phase uses the public key, client attribute list ϑ, and M_k as input to generate secret key S_k, which consists of components $G, G_i, and\ G_i'$. The secret key is generated as in Equation (3).

$$S_k = (G = g^{\frac{\delta+\vartheta}{r}}, \forall i \in \vartheta : G_i = g^r . h(i)^{r_j}\ and\ G_i' = g^{r_i}) \tag{3}$$

For each attribute $i \in \vartheta$, the algorithms select random number r and r_i with $r\ and\ r_i \in Z_p$ and h as the hash function.

Step 3 (Encryption): This process takes P_k, access policy A, and message m as input and produces the encrypted data called ciphertext (CP) as follows:

$$CP = (A, C' = m(g,g)^{\delta s}, C = h^s\ \forall x \in X: C_x = g^{\varepsilon_x}, C_{xp} = h(attribute(x)^{\varepsilon_x} \tag{4}$$

This approach generates random value s to compute shared value ε_x for each attribute in the access policy using the linear sharing of secret key. Access policy A is described through the access tree, which contains a set of nodes. The top node is the root, and the inner ones are leaf nodes or logical operators such as AND and OR. Attributes are represented in leaf node. The sample access tree is shown in Fig. 2 where the real access tree is ϑ and the access policy of A is defined as in Equation (5).

$$A = (A\ AND\ B) OR\ (C\ AND\ D) \tag{5}$$

where A is the access policy and A, B, C, and D are attributes that encrypt with CP. The decryption process must have these attributes.

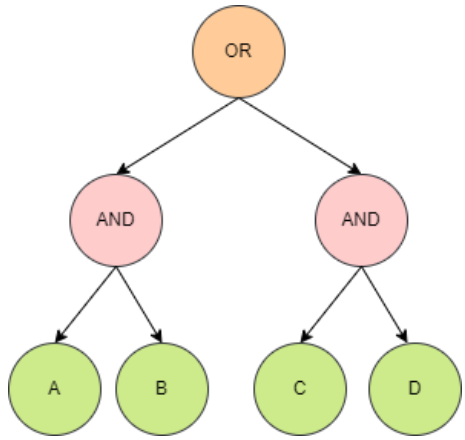

Fig. 2. Access tree to create the access policy.

Step 4 (Decryption): This process decrypts CP using secret key S_k to get the original message M as in Equation (6).

$$M = \frac{e(G_i, C_x)}{e(G_i', C_x')} \tag{6}$$

For example, if z is a leaf node, then the decryption process is performed as follows:

$$decrypt(z) = \frac{e(G_i, C_x)}{e(G_i', C_x')} \tag{7}$$

$$= \frac{e(g^r . h(i)^{r_j}, h^{\varepsilon_z})}{e(g^{r_i}, H(i)^{\varepsilon_z})} \tag{8}$$

$$= e(g, g)^{r_{\varepsilon z}} \tag{9}$$

For $i \in \vartheta$, the steps are repeated; if the attributes with secret key satisfy the access policy, then the approach decrypts the CP, otherwise the algorithm is terminated.

3.4 Cloud Network

The forwarded encrypted medical data from the edge network are stored in this central distributed storage segment that provides the services to the users of healthcare providers. This component has the responsibilities of decryption process, preprocessing, and disease prediction using a deep learning approach. The received encrypted data are decrypted using the decryption process of the LABE algorithm as stated below.

- Read the encrypted data from the LABE algorithm encryption process.
- Decrypt the data using the secret key and access policy by the cloud services.
- Transfer the decrypted data to store in the cloud for the authorized processing of disease prediction.

3.4.1 Data preprocessing

Preprocessing is important to clean the data of noise for improved classifier performance. The decrypted data are preprocessed using the normalization approach called min-max scaling. Many data mining models remain robust in data scaling, and distance-based models such as k-nearest neighbor (KNN) are

dependent on the standardization of attributes. This study utilized the common scaling method as in Equation (10) to normalize the data values.

$$d' = \frac{d - \min(D)}{\max(D) - \min(D)} \tag{10}$$

where D is the attribute vector, d is the attribute value of one sample, and d' is the scaled value of the same attribute.

3.4.2 Patient abnormality prediction using DBN-BOA

The preprocessed medical data are used for the prediction of patient illness and its severity based on the features using DBN. The deep learning models are widely used for disease prediction due to their characteristics of efficiency and accuracy. Used for a larger network structure for its faster implication, DBN consists of various hidden layers and one visible layer to provide the generalization ability. The visible layer transfers the input features into the hidden layer for prediction based on the restricted Boltzmann machine (RBM) [38]. Through the restricted hidden layer and its respective sublayers, RBM can communicate to the previous and next layers of the network. The processes in the layer are activated using the sigmoid activation function based on the RBM learning rule. The architecture of DBN is shown in Fig. 3. and it consists of stacked RBMs. RBM1 has visible and hidden layers, RBM2 has hidden layers 1 and 2, RBM3 has hidden layers 1, 2, and 3, and RBM4 consists of hidden layer 3 and one output layer.

The training of DBN includes the learning rule and parameters such as the states, each neuron bias values, and the synaptic weight. The neuron state is based on the bias and neuron weight of the previous layer, which is calculated as in Equation (11).

$$P(S_i = 1) = \frac{1}{1 + \exp(-b_i - \sum_j S_j W_{ij})} \tag{11}$$

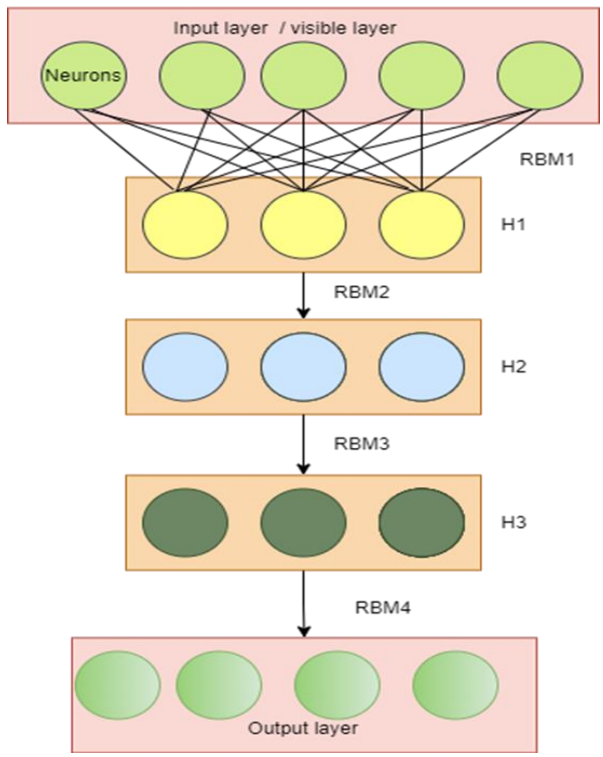

Fig. 3. Deep belief networks with stacked RBMs.

The training samples follow the positive and negative steps where the positive process converts data from the visible layer into hidden layer data and the negative process converts the data from the hidden layer into visible layer data for processing. The positive and negative steps are denoted in Equations (12) and (13) [39]. The weight is optimized as shown in Equation (14) until the maximum number of training epochs is reached. The same process has been executed to predict the abnormalities of the patients' medical data.

$$P(V_i = 1|H) = \sigma(-b_i - \sum_j H_j \mathrm{W}_{ij}) \tag{12}$$

$$P(H_i = 1|V) = \sigma(-c_i - \sum_j H_j \mathrm{W}_{ij}) \tag{13}$$

$$W' = update\left(W_{ij} + \frac{\eta}{2} \times \left(positive\left(Ed_{ij}\right) - negative\left(Ed_{ij}\right)\right)\right) \tag{14}$$

where σ is an activation function (sigmoid); $positive\left(Ed_{ij}\right)$ is positive statistics of edge $Ed_{ij} = (H_j = 1|V)$; $negative\left(Ed_{ij}\right)$ is negative statistics of edge $Ed_{ij} = P(vd_j = 1|H)$; and η is learning rate that belongs to [0,1].

The weight is optimized to avoid overfitting, and the prediction process benefits from the efficient swarm intelligence algorithm BOA. It is based on the micro bats echo location behavior where all the bats create a short, loud pulse of sound. A bat senses the object distance using the returning echo. Likewise, it can detect the difference between prey and obstacle, which allows hunting in the dark as well. A bat can randomly fly with velocity v_i in position p_i with various frequencies *f* and loudness *L* to search for prey. The frequencies are automatically adjusted, and pulse emission rate *r* depends on the target proximity [40]. Each bat in the prey listens to the other bats' voices and flies to the direction of the prey. The bat-based optimization process is defined in the following steps:

Step 1: Initialize each bat position p_i, velocity v_i, frequency f_i, loudness *L*, and pulse rate r_i. *rd1*,*rd2*, and *rd4* are the random values in the range [0,1], and *rd3* is in the range [-1,1], *t* is the iteration number, and *Lavg* is the average loudness of all the bats.

Step 2: The fitness value is evaluated.

Step 3: Do for each bat.

Step 4: Based on frequency, velocity, and locations, the new solutions are generated using Equations (15)–(17).

$$f_i = f_{min} + rd1 \times (f_{max} - f_{min}) \tag{15}$$

$$v_i = v_i + (p_i - p_{best}).f_i \tag{16}$$

$$p_i = p_i + v_i \tag{17}$$

Step 5: If $rd2 > r_i$ then

Step 6:A local solution is generated from the best possible solution as in Equation (18).

$$p_i = p_i + L_{avg} \times rd3 \tag{18}$$

End if

Step 7: If the new solution is better than the old solution and $rd4 < L_i$, then the new solution is accepted and *L* and r_i are updated as in Equations (19) and (20), respectively.

$$L_i = L_i \times 0.8 \tag{19}$$

$$r_i = r_i.(1 - \exp(-0.04 \times t) \quad (20)$$

End if

Step 8: end for

Step 9: return best bat.

3.5 Healthcare Providers

This component consists of doctors, emergency responders, and hospitals. The diagnoses resulting from the model presented in Section 3.4 are forwarded for validation to a physician. The doctors verify and confirm the results that require specific medical recommendations for the patients involved. The workflow of the proposed secure edge–cloud–IoT-based remote patient health monitoring is shown in Fig. 4. With regard to the methodologies discussed in this section, the monitoring process starts with the data collection procedure. The patients' medical data are gathered from the IoT sensors of the patients. In order to provide security of the sensitive patient data, a LABE procedure is executed in the edge network, which will be used to reduce the overhead of the cloud server and ensure low latency and response time.

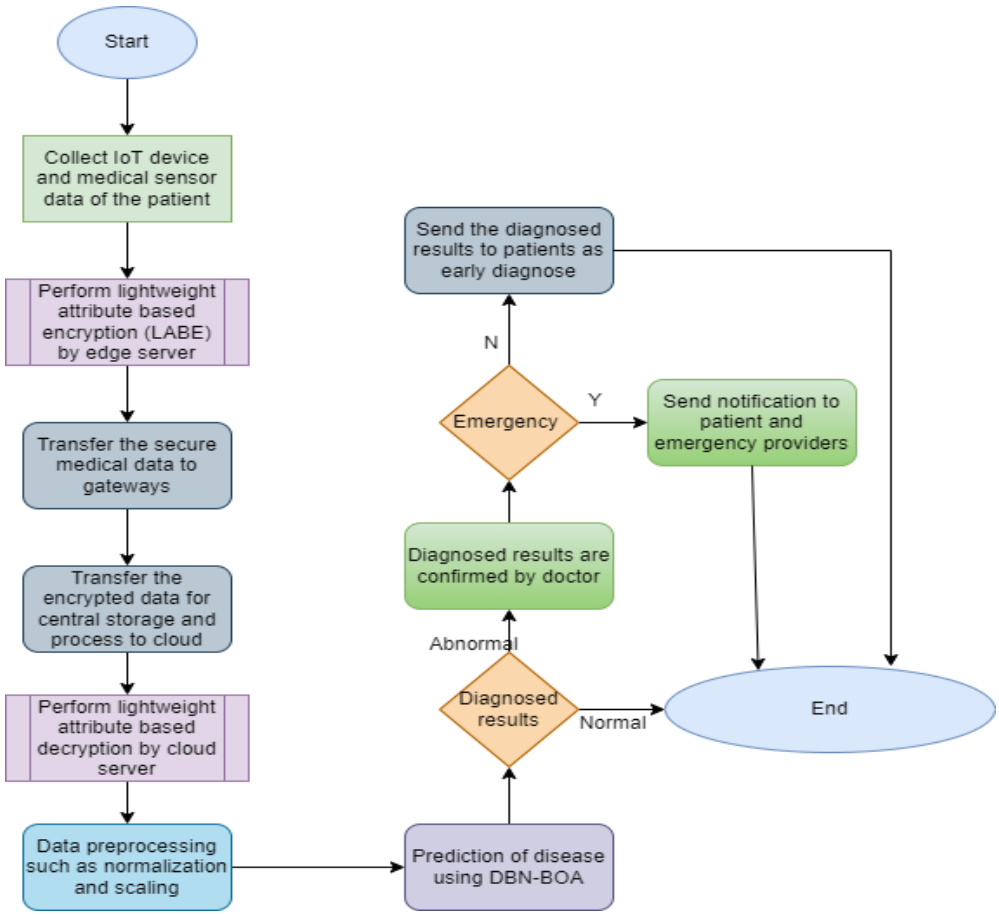

Fig. 4. Workflow of the proposed secure remote patient monitoring in edge–cloud–IoT.

The encrypted data are transferred to the cloud server for distributed storage and processing through gateways. The cloud server decrypts the data using the secret key of the LABE decryption process. The decrypted data are preprocessed to remove the noise and data scaling, which improves the accuracy of the prediction. The patient health status is predicted using DBN-BOA based on the received medical data.

Depending on the diagnosis results, the patient condition can be normal or abnormal. If it is abnormal, then the diagnosed results are once again verified by the doctor and checked if it is an emergency case or not. In emergency situations, the status of the patient is forwarded to the patient and emergency care providers. If it is not an emergency, however, then the diagnosed results are forwarded to patients for early diagnosis. Thus, the proposed remote patient healthcare monitoring system provides an efficient, secure monitoring service of the patients through IoT, edge, and cloud network.

4. Simulation Results and Discussion

The performance evaluation of the proposed remote patient health monitoring system was carried out using the medical data of healthy and unhealthy patients. The IoT environment provides an efficient platform to collect the patients' vital signs for better health monitoring, and the experiment was simulated with 300 samples. The implementation was executed in Python using scikit-learn library, with Sage math providing the execution of LABE. Evaluation metrics such as accuracy, precision, recall, and F-score were used to compare the efficiency of the proposed model with existing works using the WEKA tool by comparing the results with other classification algorithms. The samples were selected using *k*-fold cross validation, which randomly divides the data into *k* distinct fold with identical sizes. Classification was trained and tested for *k* number of times using the values 5, 10, 15, and 20 fold.

4.1 Evaluation Metrics

The proposed secure remote patient monitoring was evaluated with the following evaluation metrics:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{21}$$

$$F1 - score = \frac{TP}{TP + 1/2(FP + FN)} \tag{22}$$

$$Recall = \frac{TP}{TP + FN} \tag{23}$$

$$Precision = \frac{TP}{TP + FP} \tag{24}$$

$$False\ detection\ rate\ (FDR) = \frac{FP}{TP + TN} \tag{25}$$

The dataset is distributed in *k* folds randomly with the same number of instances. In training data, the classifier identifies the patient diseases with the normalized data. In testing data, *k*-th fold data were tested with the trained model.

4.2 Evaluation and Comparison of Classification Approaches

Figs. 5–9 illustrate the testing performance of the proposed model with other classifiers such as MLP, SVM, and CNN on the training and testing dataset using the proposed secure classification system with various cross folds. Based on the experiments, the 10-fold cross-validation results are better than other cross-fold validations for all the classifiers. The proposed deep learning-based classifier shows superior performance compared to SVM, MLP, and CNN, with CNN as second best. Comparatively, deep learning approaches obtain better outcomes than the traditional machine learning algorithms.

The best results of 10-fold cross-validations are as follows:

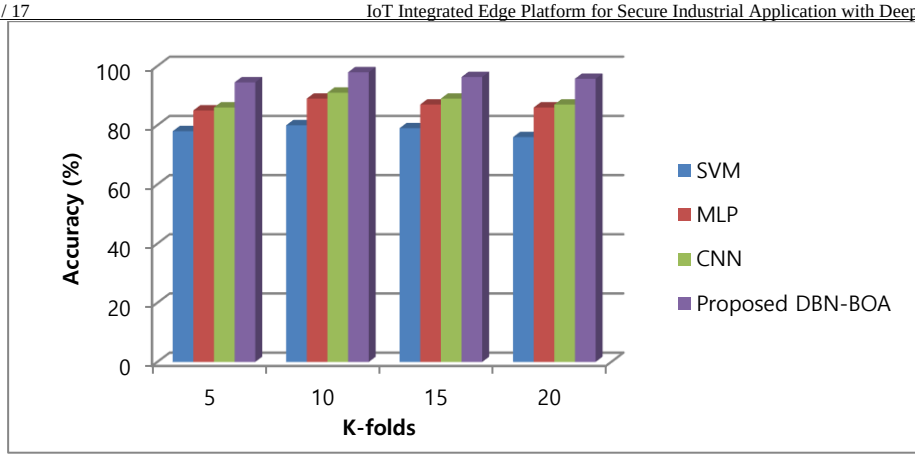

Fig. 5. Accuracy comparison of various folds between the proposed and existing classifiers.

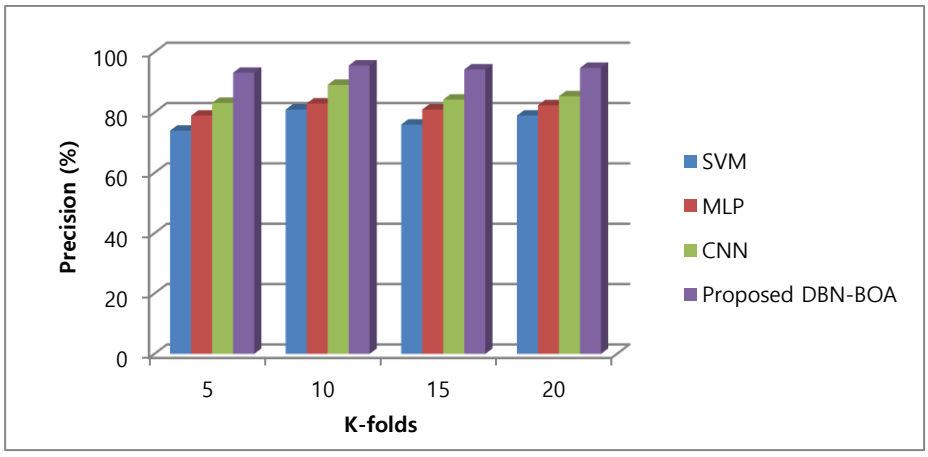

Fig. 6. Precision comparison of various folds between the proposed and existing classifiers.

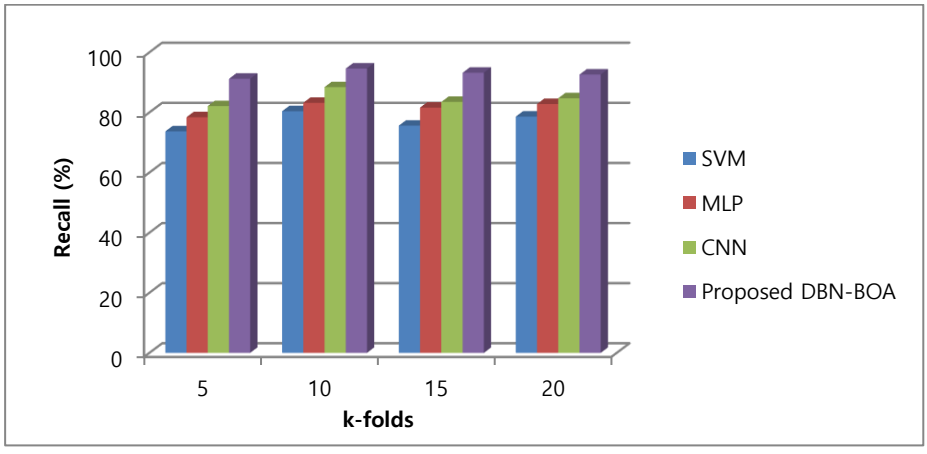

Fig. 7. Recall comparison of various folds between the proposed and existing classifiers.

- Proposed DBN-BOA: accuracy = 97.9%, precision = 95.6 %, recall = 94.6%, F1-score = 94.98%, and false detection rate (FDR) = 0.06.
- SVM: accuracy = 80%, precision = 81%, recall = 80.4%, F1-score = 82.7%, and FDR = 2.1.
- MLP: accuracy = 89%, precision = 83 %, recall = 83.2%, F1-score = 83.7%, and FDR = 1.4.

- CNN: accuracy = 91%, precision = 89.2 %, recall = 88.4%, F1-score = 88.8%, and FDR = 0.9.

The proposed deep learning-based model secured improved accuracy, precision, recall, F1-score, and reduced FDR compared to other approaches. The accuracy gain for the proposed classifier is highly likely to be attributable to the integration of the BOA algorithm.

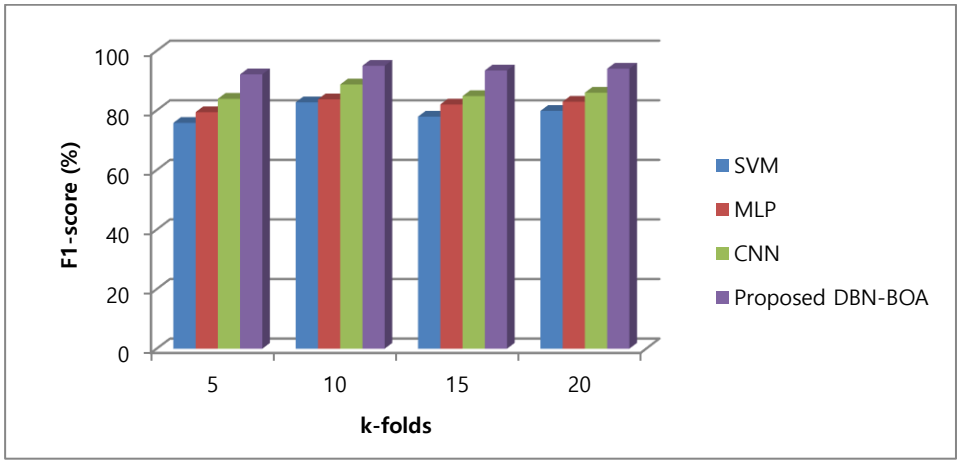

Fig. 8. F1-score comparison of various folds between the proposed and existing classifiers.

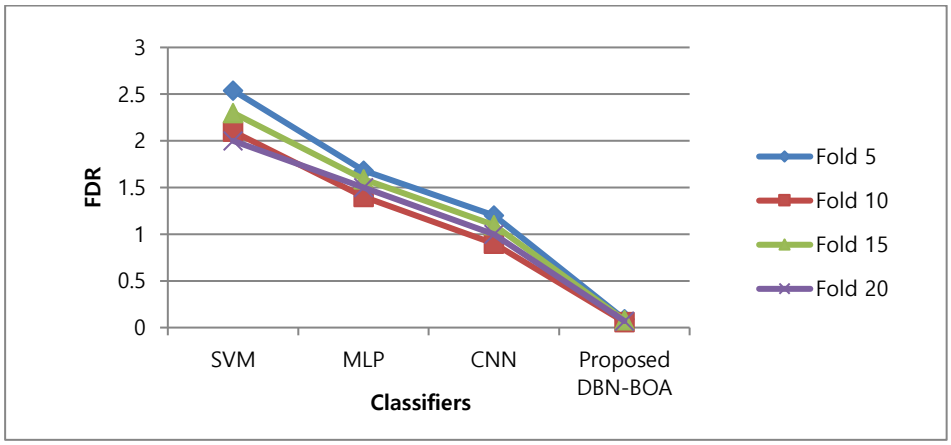

Fig. 9. FDR comparison of various folds between the proposed and existing classifiers.

4.3 Comparative Analysis of Healthcare Systems

The proposed secure edge–cloud–IoT remote healthcare system (SECIHS) was compared with the existing healthcare systems such as secure remote health monitoring system (SRHS) [5] and privacy-preserving onboard disease prediction for healthcare system (PPOHS) [6] in terms of network capacity and response time. The obtained results are shown in Table 3.

Table 3. Performance comparison of healthcare systems

Healthcare systems	Network capacity (kbps)	Response time (second)
SECIHS (proposed)	120	70
SRHS	280	130
PPOHS	270	110

It is clear from Table 3 that the proposed SECIHS requires less network capacity and less response time than the other two approaches such as SRHS and PPOHS. The proposed model obtained network capacity of 120 kbps, which is significantly smaller than SRHS (280 kbps) and PPOHS (270 kbps). In terms of response time, the proposed model obtained the best result of 70 seconds, again a considerably smaller figure than that of SRHS (130 seconds) and PPOHS (110 seconds). Utilization of edge server reduces network traffic and response time efficiently. The security aspect of the proposed healthcare system is evaluated as well in a head-to-head comparison by taking on the proposed LABE, the existing privacy-preserving self-helped diagnosis (PPSMD) [41], and the Boneh-Goh-Nissim homomorphic cryptosystem (BHC) [42]. The results are presented in Table 4.

Table 4. Performance comparison of security schemes

Security scheme type	Types of attack			
	Plaintext	Collusion	Replaying	External eavesdropping
PPSMD	No	Yes	No	Yes
BHC	Yes	No	No	Yes
Proposed LABE	Yes	Yes	Yes	Yes

The proposed security scheme is secure and is defined against plaintext, collusion, replay, and external eavesdropping attacks with secure parameters. In contrast, the other schemes provide security against plaintext attacks only, which could be easily re-launched after a period of time. Thus, the existing approaches are not suitable for providing complete security solutions for the plaintext attack. The previous approaches do not have defending capabilities, but the proposed scheme provides better security in both cloud and edge by avoiding a collusion attack. Due to the secure transmission of data, all the schemes provide security against an eavesdropping attack. The proposed security scheme provides access to policies as a significant role, which ensures protection against the replay attack and provides better security than other existing approaches. Thus, the proposed secure edge–cloud–IoT-based remote patient healthcare monitoring system ensures the security, confidentiality, and integrity of patient data and provides remote monitoring of patients for their early diagnosis.

5. Conclusion

In this study, the layered components of secure edge–cloud–IoT-based remote patient healthcare monitoring were proposed for the early diagnosis of patient disease and prediction. This proposed work incorporated a secure lightweight cryptography algorithm to ensure the security of the medical data at the edge network component. The usage of edge node before the cloud component is expected to reduce network traffic and response time. From various geographic locations, the requested data from the patients are securely processed in the cloud component. The cloud layer decrypts the data and processes it for early diagnosis. The gathered secure data are preprocessed in the cloud component prior to being used for prediction. Preprocessed medical data are classified using the proposed deep learning model called DBN-BOA optimization approach. The optimization algorithm significantly increases the accuracy of the prediction. In order to validate the performance of the proposed edge–cloud–IoT-based secure patient monitoring system, a comparative analysis of the existing classifiers and healthcare systems was performed in terms of evaluation metrics such as accuracy, precision, recall, F1-score, FDR, network capacity, and response time, based on k-fold validation on different k values. The training data are executed with *k* folds such as 5, 10, 15 and 20. The proposed algorithm secured improved accuracy (97.9%), precision (95.6%), recall (94.6%), F1-score (94.9%), and FDR (0.06) compared to other approaches. Compared to existing healthcare systems, the proposed approach required minimum network capacity (120 kbps) and response time (70 seconds). The statistical analysis proved the efficiency of the proposed healthcare system, which defends against plaintext attack, collusion attack, replay attack, and

eavesdropping attacks. Since deep learning algorithms perform much better on larger datasets, in the future, the proposed secure patient health monitoring system will be tested with a larger amount of patient data. Additionally, blockchain-based security features are planned to be executed in cloud layers for the enhanced protection of the confidentiality of patient data.

Author's Contributions

Conceptualization: SB, NB. Funding acquisition: WP. Investigation and methodology: MA, CS. Project administration: MZ. Resources: NB. Supervision: WP. Writing of the original draft: MA. Writing of the review and editing: SB, MA, CS. Software and validation: MA, MZ. Formal analysis: WP, MZ. Data curation and visualization: MZ, NB.

Funding

This work was partially supported by the Centre for Innovation and Transfer of Natural Sciences and Engineering Knowledge of the University of Rzeszow, Poland.

Competing Interests

The authors declare that they have no competing interests.

References

[1] A. Darwish, A. E. Hassanien, M. Elhoseny, A. K. Sangaiah, and K. Muhammad, "The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, pp. 4151-4166, 2019.

[2] E. Luo, M. Z. A. Bhuiyan, G. Wang, M. A. Rahman, J. Wu, and M. Atiquzzaman, "PrivacyProtector: privacy-protected patient data collection in IoT-based healthcare systems," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 163-168, 2018.

[3] S. A. Chaudhry, K. Yahya, F. Al-Turjman, and M. H. Yang, "A secure and reliable device access control scheme for IoT based sensor cloud systems," *IEEE Access*, vol. 8, pp. 139244-139254, 2020.

[4] S. A. Chaudhry, H. Alhakami, A. Baz, and F. Al-Turjman, "Securing demand response management: a certificate-based access control in smart grid edge computing infrastructure," *IEEE Access*, vol. 8, pp. 101235-101243, 2020.

[5] S. Akhbarifar, H. H. S. Javadi, A. M. Rahmani, and M. Hosseinzadeh, "A secure remote health monitoring model for early disease diagnosis in cloud-based IoT environment," *Personal and Ubiquitous Computing*, 2020. https://doi.org/10.1007/s00779-020-01475-3

[6] R. Jayaram and S. Prabakaran, "Onboard disease prediction and rehabilitation monitoring on secure edge-cloud integrated privacy preserving healthcare system," *Egyptian Informatics Journal*, vol. 22, no. 4, pp. 401-410, 2021.

[7] M. Alrazgan, "Internet of medical things and edge computing for improving healthcare in smart cities," *Mathematical Problems in Engineering*, vol. 2022, article no. 5776954, 2022. https://doi.org/10.1155/2022/5776954

[8] Y. Suryandari, "Survei IoT healthcare device," *Jurnal Sistem Cerdas*, vol. 3, no. 2, pp. 153-164, 2020. https://doi.org/10.37396/jsc.v3i2.55

[9] Y. Liu, L. Zhang, Y. Yang, L. Zhou, L. Ren, F. Wang, R. Liu, Z. Pan, and M. J. Deen, "A novel cloud-based framework for the elderly healthcare services using digital twin," *IEEE Access*, vol. 7, pp. 49088-49101, 2019.

[10] M. Ganesan and N. Sivakumar, "IoT based heart disease prediction and diagnosis model for healthcare using machine learning models," in *Proceedings of 2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN)*, Pondicherry, India, 2019, pp. 1-5.

[11] T. H. Nguyen, T. N. Nguyen, and T. T. Nguyen, "A deep learning framework for heart disease classification in an IoTs-based system," in *A Handbook of Internet of Things in Biomedical and Cyber*

Physical System. Cham, Switzerland: Springer, 2020, pp. 217-244. https://doi.org/10.1007/978-3-030-23983-1_9

[12] A. Abdelaziz, A. S. Salama, A. M. Riad, and A. N. Mahmoud, "A machine learning model for predicting of chronic kidney disease based Internet of Things and cloud computing in smart cities," in *Security in Smart Cities: Models, Applications, and Challenges*. Cham, Switzerland: Springer, 2019, pp. 93-114. https://doi.org/10.1007/978-3-030-01560-2_5

[13] H. Qiu, M. Qiu, and Z. Lu, "Selective encryption on ECG data in body sensor network based on supervised machine learning," *Information Fusion*, vol. 55, pp. 59-67, 2020.

[14] T. Zhou, J. Shen, X. Li, C. Wang, and H. Tan, "Logarithmic encryption scheme for cyber-physical systems employing Fibonacci Q-matrix," *Future Generation Computer Systems*, vol. 108, pp. 1307-1313, 2020.

[15] M. Ma, D. He, S. Fan, and D. Feng, "Certificateless searchable public key encryption scheme secure against keyword guessing attacks for smart healthcare," *Journal of Information Security and Applications*, vol. 50, article no. 102429, 2020. https://doi.org/10.1016/j.jisa.2019.102429

[16] P. Sun, "Security and privacy protection in cloud computing: discussions and challenges," *Journal of Network and Computer Applications*, vol. 160, article no. 102642, 2020. https://doi.org/10.1016/j.jnca.2020.102642

[17] A. A. Abd El-Latif, B. Abd-El-Atty, E. M. Abou-Nassar, and S. E. Venegas-Andraca, "Controlled alternate quantum walks based privacy preserving healthcare images in Internet of Things," *Optics & Laser Technology*, vol. 124, article no. 105942, 2020. https://doi.org/10.1016/j.optlastec.2019.105942

[18] A. Hassan, Y. Wang, R. Elhabob, N. Eltayieb, and F. Li, "An efficient certificateless public key encryption scheme with authorized equality test in healthcare environments," *Journal of Systems Architecture*, vol. 109, article no. 101776, 2020. https://doi.org/10.1016/j.sysarc.2020.101776

[19] M. E. Hameed, M. M. Ibrahim, N. Abd Manap, and A. A. Mohammed, "A lossless compression and encryption mechanism for remote monitoring of ECG data using Huffman coding and CBC-AES," *Future Generation Computer Systems*, vol. 111, pp. 829-840, 2020.

[20] I. Ben Dhaou, M. Ebrahimi, M. Ben Ammar, G. Bouattour, and O. Kanoun, "Edge devices for Internet of Medical Things: technologies, techniques, and implementation," *Electronics*, vol. 10, no. 17, article no. 2104, 2021. https://doi.org/10.3390/electronics10172104

[21] S. Cao, X. Lin, K. Hu, L. Wang, W. Li, M. Wang, and Y. Le, "Cloud computing-based medical health monitoring IoT system design," *Mobile Information Systems*, vol. 2021, article no. 8278612, 2021. https://doi.org/10.1155/2021/8278612

[22] Y. Zhang, G. Chen, H. Du, X. Yuan, M. Kadoch, and M. Cheriet, "Real-time remote health monitoring system driven by 5G MEC-IoT," *Electronics*, vol. 9, no. 11, article no. 1753, 2020. https://doi.org/10.3390/electronics9111753

[23] M. O. Adebiyi, M. O. Arowolo, and O. Olugbara, "A genetic algorithm for prediction of RNA-seq malaria vector gene expression data classification using SVM kernels," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 2, pp. 1071-1079, 2021.

[24] S. Gupta, L. Goel, and A. K. Agarwal, "A novel framework of health monitoring systems," *International Journal of Big Data and Analytics in Healthcare (IJBDAH)*, vol. 6, no. 1, pp. 1-14, 2021.

[25] E. T. Tan and Z. A. Halim, "Health care monitoring system and analytics based on Internet of Things framework," *IETE Journal of Research*, vol. 65, no. 5, pp. 653-660, 2019.

[26] S. Hiriyannaiah, G. M. Siddesh, M. H. M. Kiran, and K. G. Srinivasa, "A comparative study and analysis of LSTM deep neural networks for heartbeats classification," *Health and Technology*, vol. 11, no. 3, pp. 663-671, 2021.

[27] M. O. Arowolo, M. O. Adebiyi, A. A. Adebiyi, and O. Olugbara, "Optimized hybrid investigative based dimensionality reduction methods for malaria vector using KNN classifier," *Journal of Big Data*, vol. 8, article no. 29, 2021. https://doi.org/10.1186/s40537-021-00415-z

[28] M. Vahidi Farashah, A. Etebarian, R. Azmi, and R. Ebrahimzadeh Dastjerdi, "An analytics model for TelecoVAS customers' basket clustering using ensemble learning approach," *Journal of Big Data*, vol. 8, article no. 36, 2021. https://doi.org/10.1186/s40537-021-00421-1

[29] J. Jeon, J. H. Park, and Y. S. Jeong, "Dynamic analysis for IoT malware detection with convolution neural network model," *IEEE Access*, vol. 8, pp. 96899-96911, 2020.

[30] A. Makkar and J. H. Park, "SecureCPS: cognitive inspired framework for detection of cyber attacks in cyber-physical systems," *Information Processing & Management*, vol. 59, no. 3, article no. 102914, 2022. https://doi.org/10.1016/j.ipm.2022.102914

[31] E. Tcydenova, T. W. Kim, C. Lee, and J. H. Park, "Detection of adversarial attacks in AI-based intrusion detection systems using explainable AI," *Human-centric Computing and Information Sciences*, vol. 11, article no. 35, 2021. https://doi.org/10.22967/HCIS.2021.11.035

[32] N. Usman, S. Usman, F. Khan, M. A. Jan, A. Sajid, M. Alazab, and P. Watters, "Intelligent dynamic malware detection using machine learning in IP reputation for forensics data analytics," *Future Generation Computer Systems*, vol. 118, pp. 124-141, 2021.

[33] A. Lakhan, M. A. Mohammed, A. N. Rashid, S. Kadry, and K. H. Abdulkareem, "Deadline aware and energy-efficient scheduling algorithm for fine-grained tasks in mobile edge computing," *International Journal of Web and Grid Services*, vol. 18, no. 2, pp. 168-193, 2022.

[34] A. Lakhan, M. A. Mohammed, M. Elhoseny, M. D. Alshehri, and K. H. Abdulkareem, "Blockchain multi-objective optimization approach-enabled secure and cost-efficient scheduling for the Internet of Medical Things (IoMT) in fog-cloud system," *Soft Computing*, vol. 26, no. 13, pp. 6429-6442, 2022.

[35] A. Lakhan, M. A. Mohammed, J. Nedoma, R. Martinek, P. Tiwari, A. Vidyarthi, A. Alkhayyat, and W. Wang, "Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare," *IEEE Journal of Biomedical and Health Informatics*, vol. 27, no. 2, p. 664-672, 2023.

[36] M. A. Mohammed, D. A. Ibrahim, and K. H. Abdulkareem, "Bio-inspired robotics enabled schemes in blockchain-fog-cloud assisted IoMT environment," *Journal of King Saud University-Computer and Information Sciences*, vol. 35, no. 1, pp. 1-12, 2023.

[37] X. A. Wang, J. Ma, F. Xhafa, M. Zhang, and X. Luo, "Cost-effective secure E-health cloud system using identity based cryptographic techniques," *Future Generation Computer Systems*, vol. 67, pp. 242-254, 2017.

[38] G. Hinton, "A practical guide to training restricted Boltzmann machines," 2010 [Online]. Available: https://www.cs.toronto.edu/~hinton/absps/guideTR.pdf.

[39] Y. Bengio, P. Lamblin, D. Popovici, and H. Larochelle, "Greedy layer-wise training of deep networks," *Advances in Neural Information Processing Systems*, vol. 19, pp. 153-160, 2006.

[40] X. S. Yang, "A new metaheuristic bat-inspired algorithm," *Nature Inspired Cooperative Strategies for Optimization (NICSO 2010)*. Heidelberg, Germany: Springer, 2010, pp. 65-74. https://doi.org/10.1007/978-3-642-12538-6_6

[41] Y. Sun, Q. Wen, Y. Zhang, and W. Li, "Privacy-preserving self-helped medical diagnosis scheme based on secure two-party computation in wireless sensor networks," *Computational and Mathematical Methods in Medicine*, vol. 2014, article no. 214841, 2014. https://doi.org/10.1155/2014/214841

[42] W. Guo, J. Shao, R. Lu, Y. Liu, and A. A. Ghorbani, "A privacy-preserving online medical prediagnosis scheme for cloud environment," *IEEE Access*, vol. 6, pp. 48946-48957, 2018.