Journal of Autonomous Intelligence (2024) Volume 7 Issue 5
doi: 10.32629/jai.v7i5.1506

ORIGINAL RESEARCH ARTICLE

Revolutionizing healthcare with fog computing, IoT, and machine learning: An innovative framework for enhanced data security and QoS optimization

Mohit Lalit[1,*], Gaurav Bathla[1], Surender Singh[2]

[1] *Department of Computer Science and Engineering, Chandigarh University, Punjab 140413, India*

[2] *Code Quotient Pvt. Ltd. Mohali, Punjab 140413, India*

*** Corresponding author:** Mohit Lalit, mohit19862007@gmail.com

ABSTRACT

Real-time health monitoring technologies, such as fog computing (FC) and Internet of Things (IoT) sensors, have brought in a new era of healthcare. Healthcare services have accepted IoT with great ease, in accordance with Industry 4.0 goals which helped by strong fundamental components such as FC. This research uses cutting-edge technologies like fog computing and IoT to present a novel framework for meeting the changing demands of the healthcare monitoring system. With the use of machine learning, this work seeks to improve crucial communication characteristics and further the research by identifying the best security method based on the occupations of the patients. For optimisation, the framework makes use of the Firefly (FFLY) and Grey Wolf Optimisation (GWO) algorithms. Furthermore, Elliptic Curve Cryptography (ECC) and Rivest-Shamir-Adleman (RSA) encryption techniques are taken into consideration to improve data security in healthcare simulations. This security selection is powered by machine learning-based classification algorithms, where the primary goal is to maintain security while preserving energy resources. In summary, the amalgamation of the RSA security algorithm with the Firefly (FFLY) and Grey Wolf Optimization (GWO) algorithms yielded substantial enhancements in several critical Quality of Service (QoS) attributes. The proposed improved healthcare system obtains significant results in terms of QoS parameters and security selection using machine learning classification methods, surpassing the basic findings. Significantly, reliability experienced notable improvements of 17.32% and 22.69%, convergence achieved optimizations of 9.64% and 16.02%, and interoperability demonstrated improvements of 6.61% and 8.71%. Notably, when it comes to energy consumption, a vital consideration for resource-limited sensor configurations, FFLY and GWO with RSA showcased optimizations of 11.03% and 13.16%. The choice of a security algorithm is determined through machine learning techniques, where the Support Vector Machine (SVM) algorithm outperformed alternative methods. In the evaluation of classification techniques, SVM and Random Forest (RF) exhibited accuracy and F-Measure values of 0.999 and 0.993, respectively. These results underscore SVM's effectiveness in managing medical data.

Keywords: optimization; interoperability; reliability; energy consumption; machine learning

ARTICLE INFO

Received: 22 December 2023
Accepted: 18 February 2024
Available online: 15 April 2024

1. Introduction

The most significant asset in a person's life is often considered to be their health, and now almost everyone uses an array of recorded data for medications and activities to keep themselves in good health as depicted in **Figure 1**. In the recent years, according to a study presented by Al-Atawi[1], Internet of Things (IoT) enabled healthcare applications made a huge space among researchers and industry. However, energy management in low-powered sensors remains a healthcare challenge. Machine learning techniques like convolutional neural networks and fuzzy logic are widely used in healthcare for

accomplishment of various goals. Researchers are actively working on reducing energy consumption by monitoring daily activities in a health monitoring system and optimizing neural networks with efficient heuristics, as well as using fuzzy logic to extend sensor lifespans as presented by Sajedi et al.[2]. One of the techniques is widely used to reduce energy consumption is optimization algorithms based on meta heuristic approaches. Following the statement, one of the approaches, combining fuzzy logic and bio-inspired firefly algorithm presented by Uma et al.[3], effectively minimizes energy consumption in routing by prioritizing high-energy regions. However, the fusion of machine learning with cluster-based routing may help in reduction of energy consumption. And that was suggested in a cluster-based routing protocol using machine learning for Wireless Body Area Networks (WBAN) energy optimisation. Bedi et al.[4] makes use of Modified Grey Wolf Optimisation with Q-Learning. Another author Manshahia et al.[5] developed further a Grey Wolf algorithm-based method for energy-efficient routing in IoT networks with the goal of increasing network throughput while decreasing energy usage. Savanovi et al.[6] use machine learning methods, equipped with a modified Firefly algorithm to solve security issues in IoT systems for healthcare. A machine learning-driven strategy for resource optimisation in Indian healthcare using IoT data collection approach is presented by Ramaiah et al.[7]. To improve telemedicine, it creates a single platform integrating IoT, machine learning, and broadcasting units, whereas Jacob et al.[8], offers an IoT-enabled safe healthcare monitoring approach that classifies cancer using an artificial hummingbird-based CNN and secures data using a modified RSA encryption technique. Further, the study conducted by Alnaim et al.[9] offers important insights into enhancing IoT security and improving data analysis skills with potential applications for real-time systems and deep learning integration in the future. Further, another article presented by Khadidos et al.[10], introduces Random Hashing (RH) with Probabilistic Super Learning (PSL). The study conducted by Yamashita et al.[11] prioritizes healthcare treatments and patient outcomes using real-world, standardized data. The above-mentioned use cases guided the development of the optimally designed fog computing framework for e-healthcare monitoring research, while machine learning was integrated into the framework to assess the appropriate security levels based on patient professions.

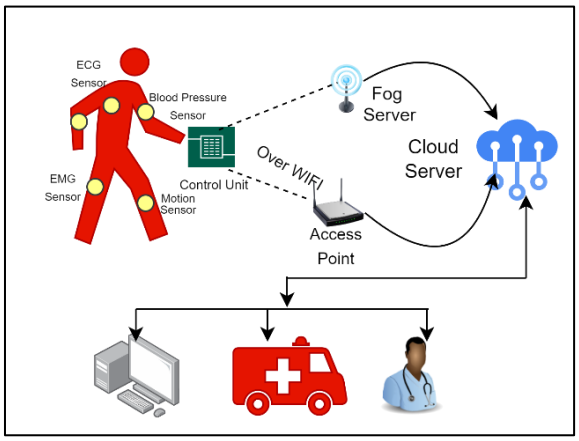

Figure 1. Fundamental healthcare monitoring framework.

The primary contribution of the paper is as follows:

1) The recently created e-healthcare monitoring frameworks are thoroughly examined, and further research gaps in the literature are identified.
2) Multi-objective optimisation techniques are provided to optimize the basic values to close such prospective research gaps.
3) The inclusion of a security mechanism when establishing communication is motivated by the lack of a security feature in the communication framework.
4) Machine learning algorithms are employed to conserve energy, and security mechanisms are selected based on the patient's profession and their device compatibility preferences, considering how well their

devices align with the existing infrastructure.

2. Related work

The development of the Internet of Things (IoT) has greatly benefited e-healthcare applications, which has led to active research activities in recent years. According to this trend, **Table 1** lists pertinent earlier investigations. A thorough analysis of E-healthcare monitoring is conducted in the table given below.

Table 1. Overview of prior research on E-Healthcare monitoring across different settings and contexts.

Ref.	Research question/objective	Methodology	Key findings/results	Contributions/significance	Limitations
[12]	Data generated by various IoT devices is encrypted depending on its importance.	Machine learning is utilized for classification, employing models like KNN, SVM, and Naïve Bayes. The approach incorporates a hybrid combination of block cipher (BC) and stream cipher (SC) to improve data security and enhance classification performance.	The proposed approach demonstrates improved CPU performance, particularly during data encryption and decryption, where efficiency is considered a critical parameter.	When utilized as one of the ML techniques for classifying security process requirements, KNN achieved a result of 76.34%.	Besides encryption/decryption and CPU time, evaluating the hybrid system's security and efficiency should also encompass crucial aspects such as memory usage, scalability, and resistance to attacks.
[13]	The suggested FC-based technique aims to use ML classification models to detect different illnesses early.	Data from IoT sensors undergoes preprocessing, computation, and classification using ML models like DT, SVM, NB, AB, RF, ANN, and K-NN.	Several classifiers are employed, and some ML classifiers, like Random Forest (RF), demonstrate superior performance by achieving maximum accuracy for heart diseases and other conditions	The RF classifier achieves impressive results for various diseases with a maximum accuracy of 97.62%, a sensitivity of 99.67%, a specificity of 97.81%, and an AUC of 99.32%.	While ML modelling is applicable, the crucial QoS parameters necessary for communication are not investigated.
[14]	The objective is to provide a framework for early identification and monitoring of lung cancer.	The approach involves using Deep Convolutional Network (DCNN) and Tasmanian Devil Hunting Optimization (TDO) for classification, enabling the identification of patterns and optimal feature selection. Additionally, the Improved Grey Wolf Algorithm (IGWO) is applied to fine-tune the parameters of the DCNN.	The suggested IGWO-based DCNN model identifies various lung disorder stages, including asthma, chronic obstructive pulmonary disease (COPD), and normal.	The suggested work has a higher specificity of 98.12% than other works, which have lower specificity percentages. The offered IGWO improves searchability, increasing lung disease prediction and reducing inaccurate prediction.	Other multi-objective optimisation methods should be investigated in addition to IGWO and TDO for optimisation.
[15]	A general, effective, and energy-conscious technique to choose the best trade-off between security needs and resource use is suggested.	The suggested method incorporates an analytical hierarchy approach (AHP) to seek for relevance between application requirement and the necessary security algorithm. The proposed approach selects best security algorithm by using knapsack problem.	Under a total energy limitation, the objective is to maximise the total utility function.	Our selection mechanism's accuracy is dependent on both the energy model and the forecast provided by the packet forecast component.	The proposed approach lacks testing in constrained device environments, despite the availability of various advanced ML algorithms for prediction these days.
[16]	The Artificial intelligence enabled healthcare monitoring framework considers QoS parameters: interoperability, convergence, reliability, and energy consumption.	Fuzzy Logic-based similarity matrix links QoS parameters using Eigenvalues and Eigenvectors concepts and MATLAB is used for simulation.	QoS parameter results: interoperability—0.761, convergence—0.438, reliability—0.251. Average energy consumption: 0.6046 (per sensor node).	The proposed healthcare framework incorporates artificial intelligence features and is simulated on 6G technology simulator enabled through MATLAB for healthcare monitoring of patients.	The proposed approach demonstrates inferior reliability and convergence values, and it also lacks a security feature in its communication framework.

Table 1. (*Continued*).

Ref.	Research question/objective	Methodology	Key findings/results	Contributions/significance	Limitations
[17]	The aim of this research is to identify BP and PPG signals and analyse the relationship between systolic blood pressure and diastolic blood pressure. This study gives an output in terms of individuals blood pressure and anxiety data.	Data is collected through E4-wristband 6 for real time monitoring through sensors placed on individuals' bodies. The stored data is then analysed, and logical stress analysis is conducted as well. The data of patients Having arterial blood pressure (ABP) and PPG is included for analysis. Various regressors are used to identify the stress and anxiety levels. Adobos Regress is used of training and testing of data.	Mean absolute error (MAE) and standard deviation (SD) of 80 patients is analysed for prediction purpose. Various repressors are used to make a comparative study for short term and long-term prediction based on BP and PPG signals.	Prediction models based on BP and PPG signals were employed for the analysis of health patients. However, this approach has not been tested yet.	The study developed a blood pressure estimation technique for healthy individuals but didn't assess its effectiveness in other patient populations. Research suggests that estimating blood pressure in obese patients is inaccurate.
[18]	The aim is to utilize Machine Learning (ML) classification algorithms to predict heart disease. This involves introducing IoMT-based cloud-fog diagnostics for heart disease.	Sensor data collected at the fog layer undergoes analysis using machine learning techniques. The analysed data is then forwarded to clinical experts for further evaluation.	The healthcare model demonstrates outstanding performance, achieving 97.32% accuracy, 97.58% recall, 97.16% precision, 97.37% F1-measure, 96.87% specificity, and 97.22% G-mean. This represents a significant advancement compared to previous models.	Various ML models, including Naïve Bayes, K-NN, Random Forest, etc., are employed, and a comparative study identifies the most suitable ML algorithm for analysis.	The ML algorithms are exclusively tested on heart disease patients, and the evaluation of the dataset necessitates testing with different analysis tools, potentially leading to diverse outcomes.
[19]	The paper aims to analyse five well-known supervised machine learning algorithms (KNN, NB, DT, RF, LR) on IoT datasets, as AI and ML play a significant role in optimizing IoT application performance with vast data generation.	The well-known ML classifier algorithms include K-Nearest Neighbours (KNN), Naive Bayes (NB), Decision Tree (DT), Random Forest (RF), and Logistic Regression (LR).	The classifiers (NB, DT, RF, KNN, and LR) are evaluated on different datasets in separate tables, comparing performance metrics such as accuracy, precision, recall, f1-score, execution time, and kappa.	The contribution is the evaluation and comparison of five well-known machine learning classifiers (NB, DT, RF, KNN, and LR) using various datasets.	The analysis only considers specific dataset variations and does not explore other factors that could impact performance, such as data preprocessing techniques, hyperparameter tuning, or ensemble methods.
[20]	The aim of this research is to optimize virtual machines in a cloud environment for healthcare applications	Implementing and evaluating three optimization methods (Cuckoo Search, Particle Swarm Optimization, and Artificial Bee Colony Optimization) to optimize virtual machines in a cloud environment for healthcare applications.	The research optimizes execution time, data processing, and system efficiency, with ABCO outperforming other algorithms at 92.7% efficiency.	This research's contribution lies in optimizing healthcare data management in a cloud-IoT environment using advanced optimization techniques, for industrial use.	The research is limited by the insufficient enhancement of the proposed system's performance. Future work should focus on improving task scheduling using varied optimization techniques and limited data processor environments.
[21]	The main goal is to create an E-Health system that enables smooth communication between patients and health providers for monitoring, diagnosis, and secure data storage, specifically focusing on heart diseases.	An optical heart rate sensor combined with amplification and noise suppression technology enables fast and accurate pulse measurements. The methodology combines hybrid meta-heuristic and mining algorithms (GWO, GA) for optimization and analysis, along with Support Vector Machine and Naïve Bayes to extract and analyse essential heart-related sensor data.	The findings indicate that SVM with the hybrid algorithm is the most effective approach for predicting heart data from IoT sensors, providing a good balance between accuracy and performance.	Numerical experiments confirm the method's effectiveness, outperforming GA and GWO in exploration and exploitation. SVM and NB, with optimization algorithms, achieve higher accuracy compared to without optimization.	The study does not explore the performance of the proposed system on a larger dataset or real-world scenarios, potentially limiting its generalizability.

The pertinent research that relates to the suggested and improved healthcare framework are included in Table It dives into current research initiatives, clarifying the use of various tools and methodologies while also addressing their limitations. Notably, the main issues with this connected work highlight the crucial points

listed below:

1) The key Quality of Service (QoS) indicators including interoperability, convergence, dependability, and energy efficiency cannot be produced by the present framework, which ensures sustainable communication[16].
2) The suggested and developed frameworks mentioned in related work lacks the security functionality[16,18].
3) The machine learning algorithms are used for various other accomplishments. Though they have not been utilized for the required level of security based on the patients' professions. To reduce information retrieval time, latency and energy usage, this assessment is highly required[18,19].

3. Proposed framework

Several healthcare services have been suggested and created, including communication tools, security features, and illness prediction based on machine learning. None of these frameworks, though, simultaneously incorporates each of these elements. Several components, including communication optimisation, the installation of security mechanisms, and the selection of the most appropriate security mechanism using machine learning classification algorithms, are used in the execution of the framework shown in **Figure 2**.

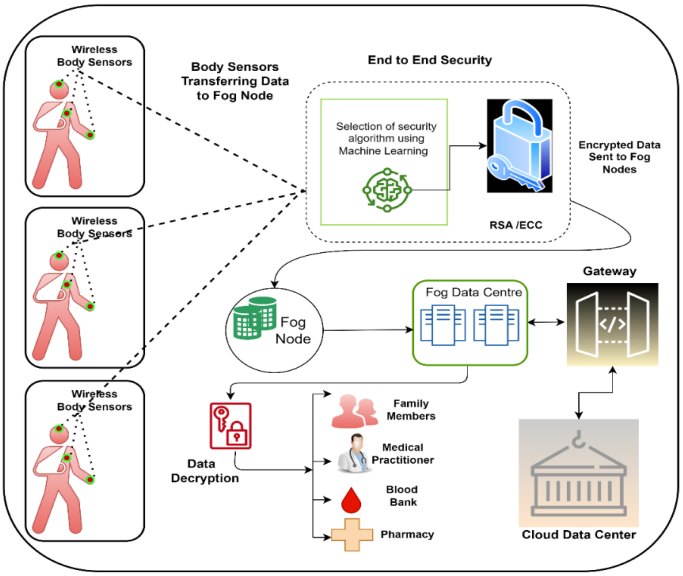

Figure 2. Proposed fog computing enabled healthcare monitoring framework.

Numerous optimisation strategies have been used over time to enhance Quality of Service (QoS) parameters. The firefly method and the grey wolf optimisation algorithm are two of the most well-known multi-objective optimisation techniques[20,21] used for attainment of numerous goals such as task scheduling, communication, optimised key size for security etc. On the flip side, the distinctive characteristics of IoT data, such as class imbalance, data volume, noise, and the presence of diverse data types, arise from various sensors. Therefore, it requires a comprehensive examination of machine learning algorithm performance within the context of these intricate IoT data characteristics.

Healthcare sensors routinely generate data, but data security remains a paramount concern. While classical and recent security mechanisms are available such as ECC[22] and RSA[23], however, not all data requires the same level of protection. For instance, ordinary individuals' health data may be transmitted to healthcare providers, whereas comparable data for prominent figures like Presidents, Prime Ministers, business magnates, and influential bureaucrats necessitates heightened security. Past healthcare frameworks lacked the provision for such selective security measures. Literature and related work analysis reveal significant gaps, notably the absence of tailored security in proposed frameworks. The existing developed frameworks often applied a uniform security process regardless of data priority type[8,24,25]. In healthcare 4.0, selecting the

appropriate security technique for data transport is essential. Few researchers, nevertheless, have concentrated on methods for choosing appropriate algorithms for limited contexts.

The optimization process of Quality of Service (QoS) parameters within the communication framework, emphasizing the critical need for data security and privacy during data transfer. However, it highlights an inherent challenge in traditional healthcare infrastructure regarding interoperability with modern security algorithms like ECC. Such advanced algorithms currently lack interoperability with conventional healthcare systems. To address this issue, RSA algorithm, despite their relatively higher power consumption compared to ECC, will be considered for ensuring security. In this scenario, the emphasis shifts towards prioritizing data transmission over energy conservation. Empirical data demonstrates that ECC offers security comparable to RSA with smaller key size. ECC provides RSA with an option by using the ECDLP for security. ECC performs well when creating digital signatures but suffers during signature verification, particularly when using larger key lengths. On the other hand, RSA decryption happens faster than ECC[26]. Therefore, RSA may be the better choice than signature generation for applications that need frequent message verification[27]. Because RSA's data verifiability is quick, it is the ideal option for medical experts who need to verify data signatures to provide expert opinions. High-end security and device interoperability are necessary for patients with important medical histories. The type of security will be provided based on following factors:

1) Security algorithm compatibility with current infrastructure and medical devices
2) Patients choose interoperable security algorithm with current infrastructure above lower energy usage.
3) The widespread adoption and implementation of RSA security algorithms over more efficient and less time-consuming ECC techniques.

Sometimes, secure data transfer and interoperability takes more priority above energy usage.

The selection of security algorithm is more important in e-healthcare-based applications and machine learning (ML) classification algorithms are used for this purpose[28]. These ML techniques have recently been employed by khadse et al.[19] for classifying data sourced from IoT devices. Patients with 'HIGH' priority should opt for ECC algorithms due to their faster encryption and energy efficiency. However, RSA, with its historical interoperability[29], may be preferred in indoor settings with stable power sources. However, ECC's reduced energy usage makes it better for outdoor applications. After identifying a significant gap in related work, the authors decided to introduce a new where, if a patient is labelled "HIGH," they should have assigned RSA with the larger key size, but standardised, interoperable on heterogeneous devices, and globally accepted security algorithm, however patients labelled "LOW" will be assigned the ECC security algorithm if interoperable and acceptable on various devices, otherwise RSA will be assigned.

4. Methodology

The QoS parameters (interoperability, convergence, reliability, energy consumption) calculated by Sodhro et al.[16] in their developed framework are not enough for a health communication under the ambit of healthcare 4.0. Another important feature is security is taken into consideration for proposed framework. The objective is of this work is to optimize these QoS parameters for a smooth functioning. Further, test the security algorithms such as RSA and ECC impact is tested for key generation and encryption decryption time. The **Figure 3** explains the working flow of FFLY and GWO algorithm.

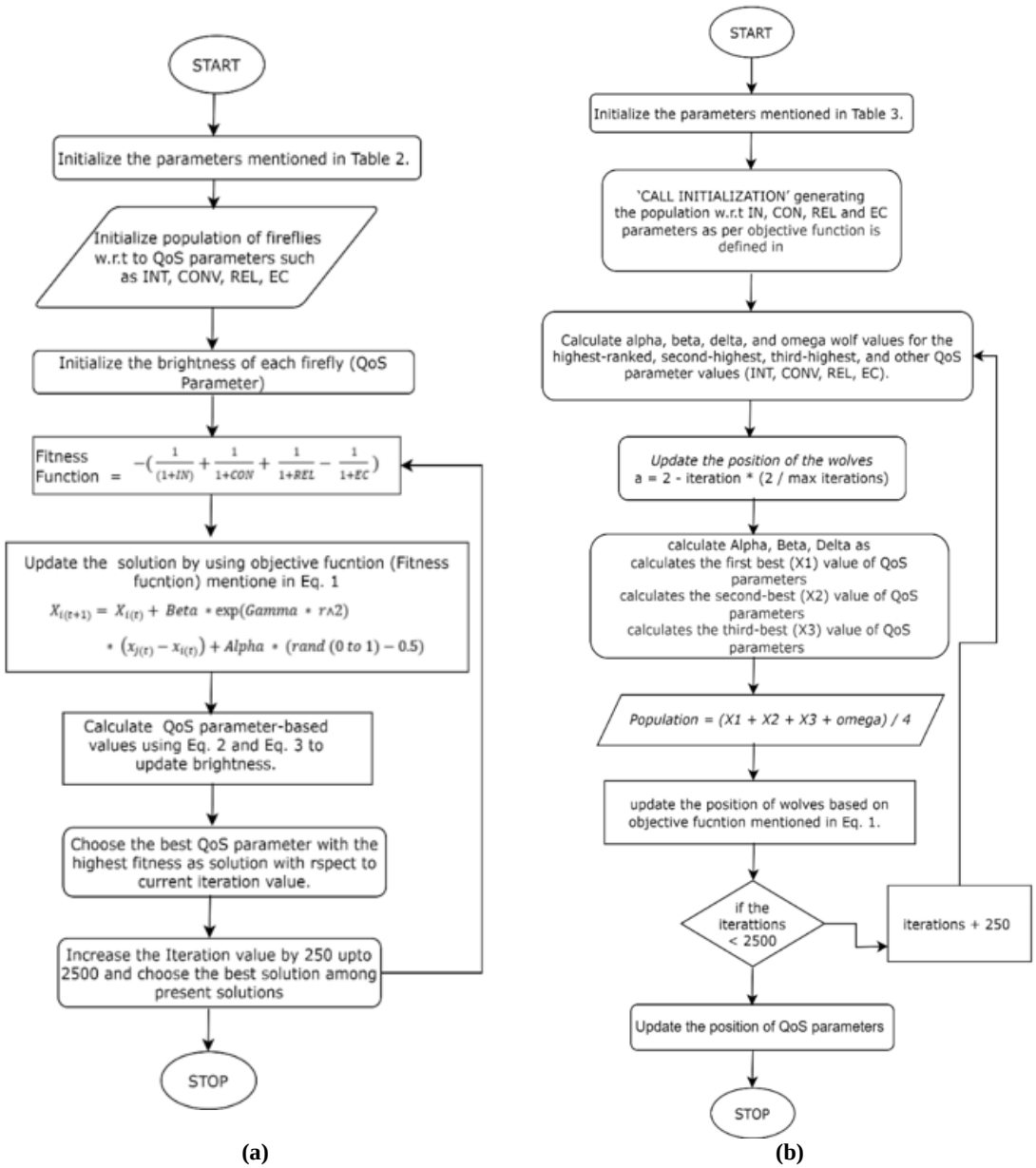

Figure 3. (a) FFLY optimization algorithm execution chart; **(b)** GWO optimization algorithm execution chart.

5. Results and analysis

The basic communication parameters driven by Sodhro et al.[16] was 0.761, 0.438, 0.251 and 0.6020 for interoperability, convergence, reliability, and energy consumption. However, while dealing with the applications like healthcare, these QoS parameters are required in their more optimal condition. To fill the both gaps, the QoS parameters are optimized with 100 population size through multi objective optimization algorithms such as firefly (FFLY) and grey wolf optimization (GWO). The simulation of these optimisation algorithms is tested with security algorithms such as RSA and ECC and the parameters used during simulation are mentioned in **Table 2**.

Table 2. Parameters used during GWO optimization.

Decision variables (*n*)	Iterations	Population size	Lower bound	Upper bound	Alpha	Beta	Delta	Omega
4	250 to 2500	50	0	1	zeros (1, *n*)	zeros (1, *n*)	zeros (1, *n*)	zeros (1, *n*)

The corresponding results are displayed in **Figure 4a–d**, where the comparison of optimized QoS parameters with FFLY and GWO are displayed. The significant improvement achieved during this simulation process.

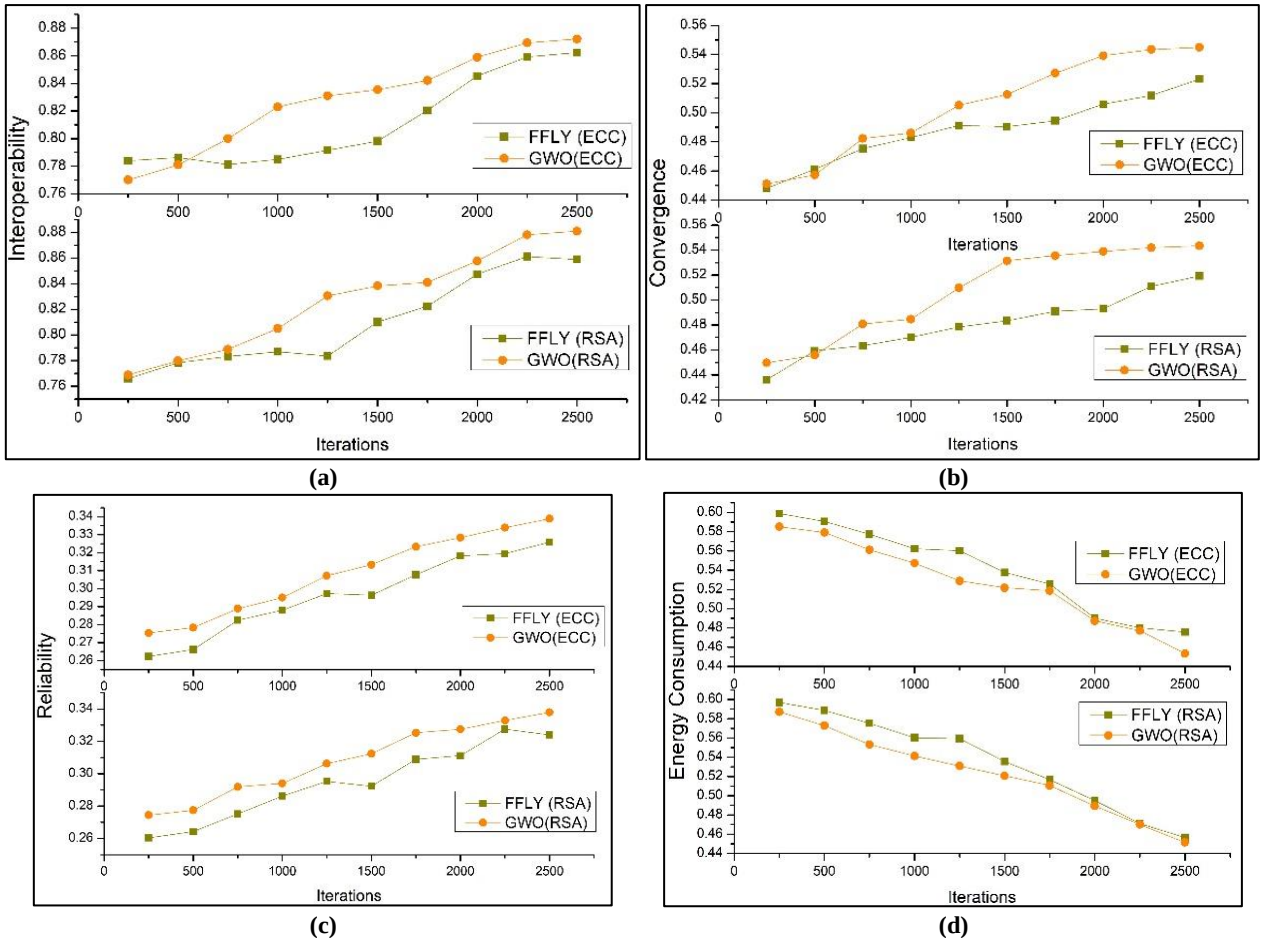

Figure 4. (a) interoperability curves on 100 dimensions; **(b)** convergence curves on 100 dimensions; **(c)** reliability curves on 100 dimensions; **(d)** energy consumption curves on 100 dimensions.

With the FFLY and GWO algorithm, embedded with RSA algorithm results in 6.61% and 8.71% improvement over input QoS parameters and FFLY and GWO algorithms embedded with ECC algorithms results in 6.87% and 8.83% improvement over input interoperability value. Similarly, FFLY and GWO with RSA algorithm produces 9.64% and 16.02% optimized results whereas, FFLY and GWO with ECC produces 11.52% and 15.27% higher results than input convergence parameter. The third parameter reliability is optimized 17.32% and 22.69% with FFLY and GWO secured with RSA algorithm, whereas the FFLY and GWO with ECC security algorithm produces 18.09% and 22.81% optimized results.

The final and the most important QoS parameter is energy consumption, which need to be minimized in such environment where sensors collecting information are constrained in nature. The optimized results of energy consumption parameter with FFLY and GWO secured with ECC are 11.03% and 13.16% and the optimized results of FFLY and GWO secured with RSA are 10.62% and 11.32%. The conclusion from above mentioned results can be drawn that the selection of security algorithm is a crucial task. The optimized results obtained with RSA produces better optimized results than ECC algorithm. The ECC security algorithm draws elliptic curve for generation of random numbers, which is a more power consuming task, whereas RSA classical algorithm has less calculative complexities than ECC algorithm.

The primary objective of this result section is the optimisation, which achieved the interoperability parameter optimized using FFLY and GWO. The GWO algorithm achieved higher optimized values than the

FFLY method. Other factors, such as convergence and reliability, are also optimized, with the GWO algorithm outperforming the FFLY method, as seen in **Figure 4a–c**. The fourth but not least parameter is energy usage in relation to the security method applied during communication. As seen in **Figure 4d**, the energy use was lower when ECC was used instead of RSA during simulation. However, given to its compatibility and global acceptability, RSA has an advantage over ECC.

The comparison of results based on depicted in **Figure 5a–d** with base values (BV) taken from Manshahia et al.[1]. The optimized results using FFLY and GWO algorithm can been seen for various QoS parameters. The standard scaling of QoS parameters vary between 0 to 1, however in case of optimization of QoS parameters such as interoperability, convergence and reliability needs to vary towards 1. The more these values will vary towards 1, the more performance of framework will rise. In case of minimization of QoS parameters, such as energy consumption, the parametric values need to go decline side towards 0, which ensures the less energy consumption during communication.

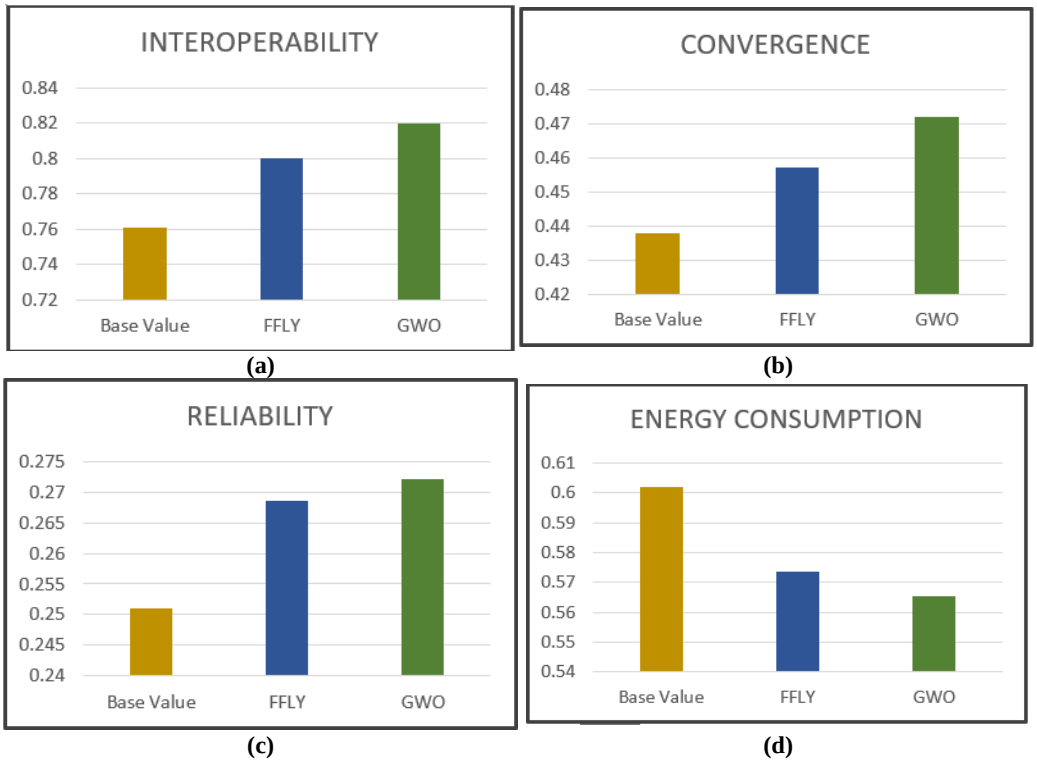

Figure 5. (a) comparison of interoperability with BV; **(b)** comparison of convergence with BV; **(c)** comparison of reliability with BV; **(d)** comparison of energy consumption with BV.

The next part of result section focuses on determining the appropriate security mechanism based on globally acceptability and interoperability features using machine learning-based classification algorithms.

As previously stated, machine learning classification algorithms can be used for classification. The dataset used for classification has been sourced from U.S. Department of Health & Human Services. Centres for Disease Control and Prevention[30], incorporating key parameters like Year Start, Year End, Location, Data Source, Topic, and the newly introduced 'Priority' field. This field is intended to categorize patients, who are grappling with chronic and severe ailments. Notably, an added layer is established for patient classification based on their 'Priority' designation. The dataset segregates patients into 'LOW' and 'HIGH' priority classes based on their parameters. This classification strategy guides the selection of appropriate security algorithms. For patients classified as 'LOW' priority, a security algorithm like ECC is opted for, striking a balance between computational efficiency and security. Conversely, patients assigned 'HIGH' priority receive a more secure but computationally expensive encryption method such as RSA due to its interoperability feature and global

acceptance[26]. This tailored approach optimizes energy consumption and prolongs sensor operational duration. Prominent ML classifiers like NB, K-NN, and SVM[31,32] WEKA tool[33].

Assessment of Classifier Performance: The effectiveness of the three classifiers is measured using four metrics. Below are the details of the evaluation criteria.

1) Accuracy: This assesses the overall classifier performance.

$$\text{Accuracy} = ((T\_postv + T\_negtv)/(T\_postv + F\_postv + T\_negtv + F\_negtv)) \times 100\%$$

2) Sensitivity: Sensitivity, also known as precision, is the ratio of true positive cases to the total number of cases affected by the disease. The sensitivity is evaluated as

$$\text{Sensitivity} = (T\_postv/(T\_negtv + F\_negtv)) \times 100\%$$

3) Specificity: It quantifies the proportion of accurate negative cases out of the total affected by the disease.

$$\text{Specificity: } (T\_negtv/(T\_negtv + F\_postv)) \times 100\%$$

4) AUC: This graphical comparison illustrates the true and false positive rates, with a greater AUC value being deemed superior.

where T_postv (TP) and T_negtv (TN) denote the healthcare model's accurate positive and negative predictions, and F_postv (FP) and F_negtv (FN) represent the healthcare model's incorrect positive and negative predictions. The dataset and its corresponding attributes are presented in **Table 3**.

Table 3. Dataset and its attributes.

Data set reference	Size	Instance	Feature	Data type	Null values	Data split (training: test)
[2]	22.5 kB	500	7	Binary	None	70:30

Table 4. Various machine learning algorithms-based data classification results for data set[32].

SVM			**NB**			**K-NN**		
A	36	0	A	21	15	A	30	6
B	0	114	B	41	73	B	4	110
	A	B		A	B		A	B
Correctly Classified Instances		99.98%	Correctly Classified Instances		61.1 %	Correctly Classified Instances		93.33%
Incorrectly Classified Instances		0.67%	Incorrectly Classified Instances		38.9%	Incorrectly Classified Instances		6.67%
DT			**RF**					
A	35	1	A	35	1			
B	0	114	B	0	114			
	A	B		A	B			
Correctly Classified Instances		99.11%	Correctly Classified Instances		99.33%			
Incorrectly Classified Instances		0.89%	Incorrectly Classified Instances		0.67%			

The results of various classification techniques are displayed in the above-mentioned **Table 4**. The results are based on various machine learning based classification techniques such as NB, SVM, K-NN, RD, DT. The classification of patients with 'LOW' and 'HIGH' priority is decided based on the level of required security to that patient. The security algorithm selection among ECC and RSA will be decided based on their profession. The classification done for this purpose is presented in **Table 4** and the corresponding comparison of various present classification techniques are presented in **Figure 5a–d**.

Table 3 and **Figure 6** clearly show that the Support Vector Machine (SVM) method surpasses all other categorization algorithms. This claim is supported by the related confusion matrix, which consistently demonstrates SVM's higher performance. For evaluation, key classification metrics such as True Positive Rate (Tpostv), False Positive Rate (Fpostv), Precision, and F-measures were rigorously recorded and presented in

Figure 5. SVM outperformed Nave Bayes (61.1%), k-Nearest Neighbours (83.3%), Random Forest (99.3%), and Decision Trees (98.27%) in terms of TP rate. SVM, on the other hand, excelled in FP rate with only 0.2%, proving its great accuracy and little misclassification. As a result, SVM is unquestionably the best method, followed in descending order by RF, DT, k-NN, and NB.

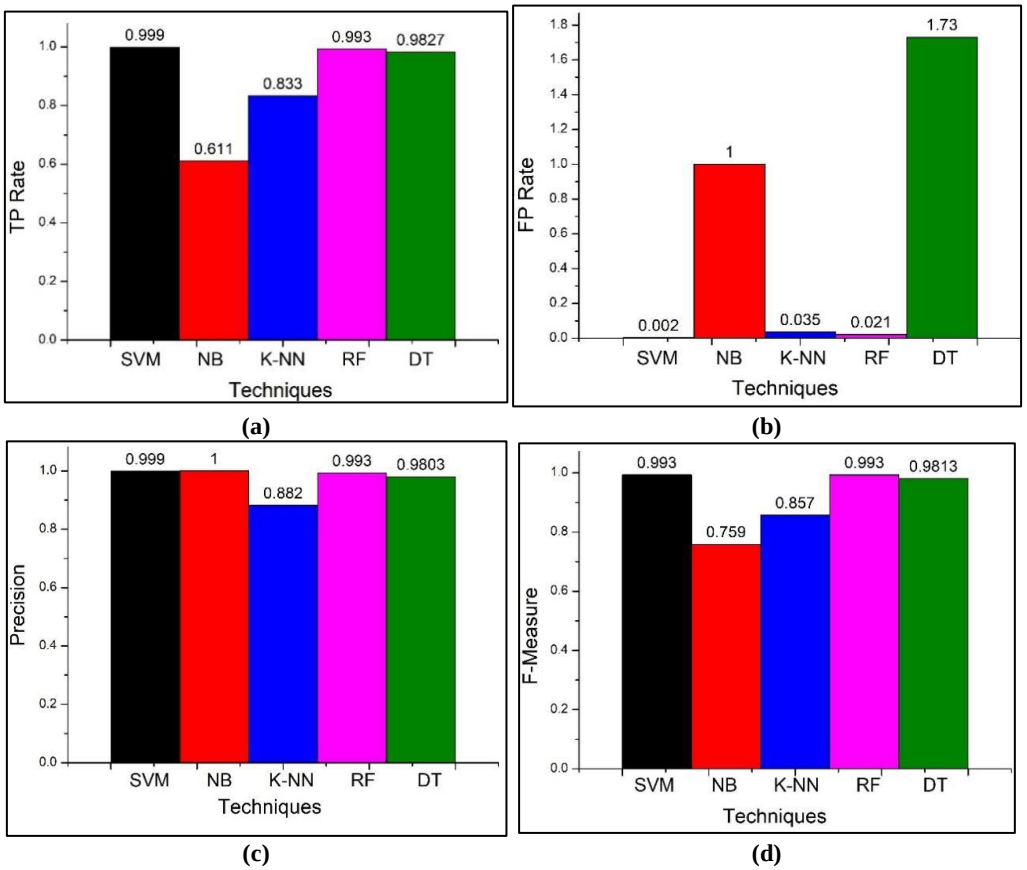

Figure 6. Performance comparison of various machine learning based classification Algorithms.

Precision and F-Measure are important measures for assessing prediction quality, particularly in contexts such as medical datasets. Precision measures the precision of positive classifications, demonstrating how many are truly positive. The F-Measure, on the other hand, integrates both recall and accuracy, revealing how many true positives were accurately detected in a single operation, making it useful for establishing a balance between both aspects. The graphs in **Figure 6** show that Nave Bayes (NB) has the highest accuracy rate, whereas SVM, k-Nearest Neighbours (k-NN), Random Forest (RF), and Decision Trees (DT) have precision rates of 0.999, 0.882, 0.993, and 0.9803, respectively. Furthermore, in terms of F-Measure parameters, SVM and RF reach the greatest value of 0.993, while NB, k-NN, and DT achieve 0.759, 0.857, and 0.9813, respectively. These criteria are critical in determining the efficacy of categorization algorithms, especially in the context of medical data processing. This is especially important since energy conservation is a critical concern in settings where sensors have limited power resources and the selection of right security algorithm (either RSA or ECC) can save significant amount of energy, as depicted in **Figure 4d**. However, energy saving can be place on second position when it comes to ensuring the timely transmission of data for persons who are most important.

The existing framework that lacked a security mechanism has a significant disadvantage compared to the recently introduced and improved framework. The addition of a classification system based on machine learning has also added advantage to this work. This method is used to intelligently select the proper security measures, resulting in more effective energy conservation.

6. Conclusion and future directions

This study introduces a healthcare framework that uses FFLY and GWO to track patients' health. The FFLY and GWO algorithm's fundamental function is to facilitate communication across heterogeneous devices, which must be highly interoperable for effective communication. The framework has been refined to the point that it can offer an interoperable, reliable, convergent, and energy-efficient environment for monitoring patient health. With the aid of multi-objective optimisation algorithms like FFLY and GWO, the best value for each performance indicator is selected from the population of randomly generated data. The new framework outperforms the basic findings in terms of interoperability, convergence, dependability, and energy usage. The outcomes analysis, where FFLY and GWO both adjust the performance parameters, is shown in Section 5. The generation of the random population is done to choose the best values of the performance parameters. The optimised results are better than the base values and are 9.76%, 16.36%, 23.09%, and 12.62% for interoperability, convergence, dependability, and energy consumption, respectively. Whereas in terms of security, ECC surpasses RSA in terms of encryption time, decryption time, and key size in the simulation using the security features of ECC and RSA. The primary need for a framework with fog computing capabilities is that all ECC security measures use less energy when compared to RSA. Machine learning principles can be applied to the selection of suitable data security methods for future usage.

Author contributions

Conceptualization, ML and GB; methodology, ML; software, GB; validation, ML, GB and SS; formal analysis, ML; investigation, ML and GB; resources, ML; data curation, GB; writing—original draft preparation, ML and SS; writing—review and editing, ML, GB and SS; visualization, ML; supervision, GB and SS; project administration, GB. All authors have read and agreed to the published version of the manuscript.

Acknowledgments

Here, you can acknowledge any support given which is not covered by the author contribution or funding sections. This may include administrative and technical support, or donations in kind (e.g., materials used for experiments).

Conflict of interest

The authors declare no conflict of interest.

References

1. Al-Atawi AA, Khan F, Kim CG. Application and Challenges of IoT Healthcare System in COVID-19. Sensors. 2022; 22(19): 7304. doi: 10.3390/s22197304
2. Sajedi SN, Maadani M, Nesari Moghadam M. F-LEACH: a fuzzy-based data aggregation scheme for healthcare IoT systems. The Journal of Supercomputing. 2021; 78(1): 1030-1047. doi: 10.1007/s11227-021-03890-6
3. Deepak BBVL, Bahubalendruni MVAR, Parhi DRK, et al. Intelligent Manufacturing Systems in Industry 4.0. Springer Nature Singapore; 2023. doi: 10.1007/978-981-99-1665-8
4. Bedi P, Das S, Goyal SB, et al. A novel routing protocol based on grey wolf optimization and Q learning for wireless body area network. Expert Systems with Applications. 2022; 210: 118477. doi: 10.1016/j.eswa.2022.118477
5. Manshahia MS. Grey Wolf Algorithm based Energy-Efficient Data Transmission in Internet of Things. Procedia Computer Science. 2019; 160: 604-609. doi: 10.1016/j.procs.2019.11.040
6. Savanović N, Toskovic A, Petrovic A, et al. Intrusion Detection in Healthcare 4.0 Internet of Things Systems via Metaheuristics Optimized Machine Learning. Sustainability. 2023; 15(16): 12563. doi: 10.3390/su151612563
7. Ramaiah NS, Ahmed ST. An IoT-Based Treatment Optimization and Priority Assignment Using Machine Learning. ECS Trans, 107(1), 1487–1495. doi: 10.1149/10701.1487ECST/META
8. Jacob TP, Pravin A, Kumar RR. A secure IoT based healthcare framework using modified RSA algorithm using an artificial hummingbird-based CNN. Transactions on Emerging Telecommunications Technologies. 2022;

33(12). doi: 10.1002/ett.4622
9. Alnaim AK, Alwakeel AM. Machine-Learning-Based IoT–Edge Computing Healthcare Solutions. Electronics. 2023; 12(4): 1027. doi: 10.3390/electronics12041027
10. Khadidos AO, Shitharth S, Khadidos AO, et al. Healthcare Data Security Using IoT Sensors Based on Random Hashing Mechanism. Papageorgas P, ed. Journal of Sensors. 2022; 2022: 1-17. doi: 10.1155/2022/8457116
11. Yamashita T, Wakata Y, Nakaguma H, et al. Machine learning for classification of postoperative patient status using standardized medical data. Computer Methods and Programs in Biomedicine. 2022; 214: 106583. doi: 10.1016/j.cmpb.2021.106583
12. Khwailleh D, Al-balas F. A dynamic data encryption method based on addressing the data importance on the internet of things. International Journal of Electrical and Computer Engineering (IJECE). 2022; 12(2): 2139. doi: 10.11591/ijece.v12i2.pp2139-2146
13. Kishor A, Chakraborty C. Artificial Intelligence and Internet of Things Based Healthcare 4.0 Monitoring System. Wireless Personal Communications. 2021; 127(2): 1615-1631. doi: 10.1007/s11277-021-08708-5
14. Irshad RR, Hussain S, Sohail SS, et al. A Novel IoT-Enabled Healthcare Monitoring Framework and Improved Grey Wolf Optimization Algorithm-Based Deep Convolution Neural Network Model for Early Diagnosis of Lung Cancer. Sensors. 2023; 23(6): 2932. doi: 10.3390/s23062932
15. Taddeo AV, Ferrante A. Run-time selection of security algorithms for networked devices. Proceedings of the 5th ACM symposium on QoS and security for wireless and mobile networks. Published online October 28, 2009. doi: 10.1145/1641944.1641963
16. Sodhro AH, Zahid N. AI-Enabled Framework for Fog Computing Driven E-Healthcare Applications. Sensors. 2021; 21(23): 8039. doi: 10.3390/s21238039
17. Alazzam MB, Alassery F, Almulihi A. A Novel Smart Healthcare Monitoring System Using Machine Learning and the Internet of Things. Rani S, ed. Wireless Communications and Mobile Computing. 2021; 2021: 1-7. doi: 10.1155/2021/5078799
18. Kishor A, Chakraborty C, Jeberson W. Intelligent healthcare data segregation using fog computing with internet of things and machine learning. International Journal of Engineering Systems Modelling and Simulation. 2021; 12(2/3): 188. doi: 10.1504/ijesms.2021.115533
19. Khadse V. An empirical comparison of supervised machine learning algorithms for internet of things data. Fourth International Conference on Computing Communication. Available online: https://ieeexplore.ieee.org/abstract/document/8697476/?casa_token=SqliZQlQhG4AAAAA:i21wkyY8TH0p9aUxNO_sCY6gxuJdCeon9dD7IWcJyWXfty_J8zp-qhV84PoSkjh1lQikILg (accessed on 29 June 2023).
20. Watanabe O, Zeugmann T, eds. Stochastic Algorithms: Foundations and Applications. Springer Berlin Heidelberg; 2009. doi: 10.1007/978-3-642-04944-6
21. Mirjalili S, Song Dong J, Lewis A, et al. Nature-Inspired Optimizers. Springer International Publishing; 2020. doi: 10.1007/978-3-030-12127-3
22. Vanstone SA. Elliptic curve cryptosystem—The answer to strong, fast public-key cryptography for securing constrained environments. Information Security Technical Report, 2(2), 78–87. doi: 10.1016/S1363-4127(97)81331-3
23. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM. 1978; 21(2): 120-126. doi: 10.1145/359340.359342
24. Suárez-Albela M, Fraga-Lamas P, Fernández-Caramés T. A Practical Evaluation on RSA and ECC-Based Cipher Suites for IoT High-Security Energy-Efficient Fog and Mist Computing Devices. Sensors. 2018; 18(11): 3868. doi: 10.3390/s18113868
25. Mahto D, Khan D. Security analysis of elliptic curve cryptography and RSA. Available online: http://www.iaeng.org/publication/WCE2016/WCE2016_pp419-422.pdf (accessed on 6 October 2023).
26. Perez GM, Tiwari S, Trivedi MC, et al. Ambient Communications and Computer Systems. Springer Singapore; 2018. doi: 10.1007/978-981-10-7386-1
27. Mousavi SK, Ghaffari A, Besharat S, et al. Security of internet of things based on cryptographic algorithms: a survey. Wireless Networks. 2021; 27(2): 1515-1555. doi: 10.1007/s11276-020-02535-5
28. Vahdati Z, Ghasempour A, Salehi M, et al. Comparison of ECC and RSA algorithms in IoT devices. Article in Journal of Theoretical and Applied Information Technology. 2019; 31: 16.
29. Boneh D, Shacham H. Fast variants of RSA. CryptoBytes. 2002; 5(1): 1-9.
30. U.S. Department of Health & Human Services. Centers for Disease Control and Prevention. 2021.
31. Kishor A, Chakraborty C, Jeberson W. Reinforcement learning for medical information processing over heterogeneous networks. Multimedia Tools and Applications. Published online March 29, 2021. doi: 10.1007/s11042-021-10840-0
32. Singh PK, Wierzchoń ST, Tanwar S, et al. Proceedings of Second International Conference on Computing, Communications, and Cyber-Security. Springer Singapore; 2021. doi: 10.1007/978-981-16-0733-2
33. Weka 3: Data Mining Software in Java. Available online: https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Weka+3%3A+Data+Mining+Software+in+Java.+http%3A%2F%2Fwww.cs.waikato.ac.nz%2Fml%2Fweka%2F%2C+Accessed+13+July+2017&btnG= (accessed on 10 August 2023).