

Article

A Novel Approach for Improving the Security of IoT–Medical Data Systems Using an Enhanced Dynamic Bayesian Network

Mohammed Amin Almaiah ^{1,2,*}, Sandeep Yelisetti ³, Leena Arya ⁴, Nelson Kennedy Babu Christopher ⁵, Kumaresan Kaliappan ⁶, Pandimurugan Vellaisamy ⁷, Fahima Hajje ⁸  and Tayseer Alkdour ⁹

¹ College of Information Technology, Aqaba University of Technology, Aqaba 11947, Jordan

² Applied Science Research Center, Applied Science Private University, Amman 11931, Jordan

³ Department of IT, V R Siddhartha Engineering College, Vijayawada 520007, India

⁴ Department of CSE, Koneru Lakshmaiah Education Foundation, Mangalagiri, Vaddeswaram 522502, India

⁵ Department of Computer Science and Engineering, Saveetha School of Engineering, Chennai 602105, India

⁶ Maratsolutions, Coimbatore 641001, India

⁷ School of Computing, Department of Networking and Communications, SRM Institute of Science & Technology, Kattankulathur Campus, Chennai 603203, India

⁸ Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia

⁹ College of Computer Science and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia

* Correspondence: m.almaayah@aau.edu.jo

Abstract: IoT (Internet of Things) devices are increasingly being used in healthcare to collect and transmit patient data, which can improve patient outcomes and reduce costs. However, this also creates new challenges for data security and privacy. Thus, the major demand for secure and efficient data-sharing solutions has prompted significant attention due to the increasing volume of shared sensor data. Leveraging a data-fusion-based paradigm within the realm of IoT-protected healthcare systems enabled the collection and analysis of patient data from diverse sources, encompassing medical devices, electronic health records (EHRs), and wearables. This innovative approach holds the potential to yield immediate benefits in terms of enhancing patient care, including more precise diagnoses and treatment plans. It empowers healthcare professionals to devise personalized treatment regimens by amalgamating data from multiple origins. Moreover, it has the capacity to alleviate financial burdens, elevate healthcare outcomes, and augment patient satisfaction. Furthermore, this concept extends to fortifying patient records against unauthorized access and potential misuse. In this study, we propose a novel approach for secure transmission of healthcare data, amalgamating the improved context-aware data-fusion method with an emotional-intelligence-inspired enhanced dynamic Bayesian network (EDBN). The findings indicated that F1 score, accuracy, precision, recall, and ROC-AUC score using DCNN were 89.3%, 87.4%, 91.4%, 92.1%, and 0.56, respectively, which was second-highest to the proposed method. On the other hand, the F1 score, accuracy, precision, recall, and ROC-AUC scores of FRCNN and CNN were low in accuracy at 83.2% and 84.3%, respectively. Our experimental investigation demonstrated superior performance compared with existing methods, as evidenced by various performance metrics, including recall, precision, F measures, and accuracy.

Keywords: IoT–medical network; data security; IoT–medical security; emotional intelligence; EDBN



Citation: Almaiah, M.A.; Yelisetti, S.; Arya, L.; Babu Christopher, N.K.; Kaliappan, K.; Vellaisamy, P.; Hajje, F.; Alkdour, T. A Novel Approach for Improving the Security of IoT–Medical Data Systems Using an Enhanced Dynamic Bayesian Network. *Electronics* **2023**, *12*, 4316. <https://doi.org/10.3390/electronics12204316>

Academic Editor: Juan-Carlos Cano

Received: 3 September 2023

Revised: 10 October 2023

Accepted: 13 October 2023

Published: 18 October 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Emotional intelligence healthcare merges technology and AI with a focus on empathizing with patients' emotions. By utilizing sophisticated algorithms and data analysis, it enables medical professionals to gain insights into patient behaviors and improve their quality of care. This approach not only leads to personalized treatment but also aids in identifying potential mental health and medical problems before they escalate, ultimately reducing healthcare costs [1].

Fusion-based healthcare systems in IoT environments combine various data sources, such as patient data, medical records, and photographs, to provide a comprehensive view of a patient's health [2]. This approach allows medical professionals to understand a patient's medical history, current health, and potential future health risks. Real-time monitoring of patient health is also made possible through this integration, enabling prompt identification and treatment of medical issues. By utilizing sensors and devices connected to the IoT, the system gathers data from multiple sources and fuses it into one complete picture, as shown in Figure 1. This data fusion offers valuable insights to healthcare providers, aiding in informed decision making for a patient's care. Additionally, the system offers advanced analytical capabilities, allowing healthcare professionals to detect patterns in patient data, anticipate future health problems, and optimize treatment plans [3].

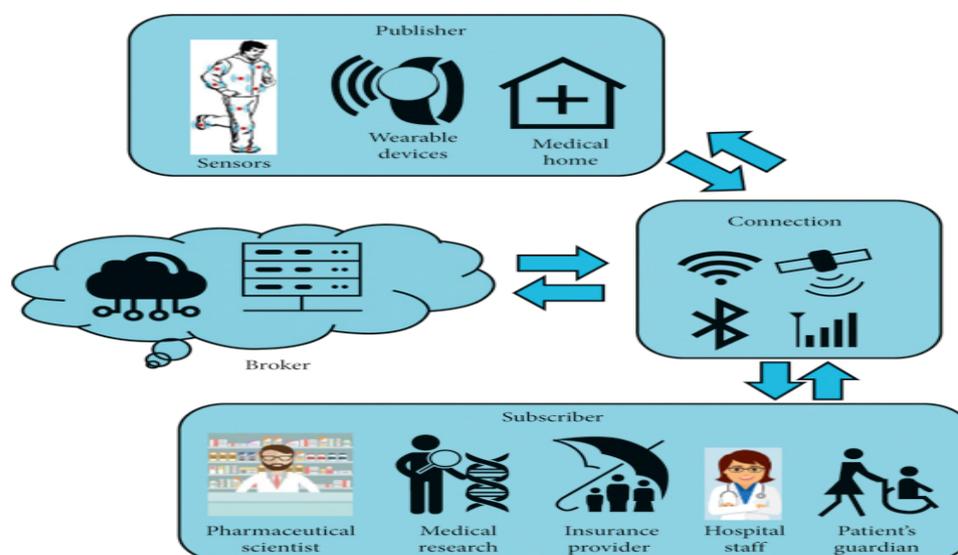


Figure 1. IoT with AI based Healthcare System.

Emotional intelligence is being incorporated into healthcare to protect data collected by IoT devices. By considering the human element and security aspect, this concept can detect anomalies and threats to data security. It can also identify unusual user behavior to prevent malicious activity. This approach not only enhances data security, but also ensures its reliability [4].

IoT (Internet of Things) devices are increasingly being used in healthcare to collect and transmit patient data, which can improve patient outcomes and reduce costs. However, this also creates new challenges for data security and privacy. Here are some ways that IoT devices can be used to enhance the security of healthcare data [5]:

Encryption: IoT devices should use encryption to secure data transmission and storage. This implies that data are encoded in a way that only authorized parties may decode.

Authorization and Authentication: In order to guarantee that only authorized users may access and alter data, devices should utilize authentication and authorization protocols. This can be done using methods such as passwords, biometrics, or smart cards.

Data Access Control: Access to patient data should be restricted to authorized personnel only. This can be done by implementing role-based access control, where each user is granted access to data based on their role and level of authorization.

Regular Auditing: Regular auditing of the IoT system can help identify any security vulnerabilities and monitor user activity. This can be done through system logs, alerts, and reports.

Data-sharing issues in healthcare systems have been a long-standing challenge due to concerns around data privacy, security, and ownership. Fusion-based approaches, which combine data from multiple sources to provide more comprehensive and accurate insights, can exacerbate these issues if not handled appropriately. Emotional intelligence (EI) can

play a critical role in addressing these issues by enabling healthcare providers to understand and manage the emotional aspects of data sharing and privacy concerns [6]. Fusion-based procedures sometimes include merging data from many sources, such as electronic health records (EHRs), to give a more complete picture of a patient's health, medical devices, and patient-generated data. However, there may be substantial problems with data security and privacy due to this connection [7]. One illustration is that the exchange of patient data between healthcare professionals may be limited by legal and ethical considerations, which can lead to a lack of data sharing between healthcare providers. This, in turn, can impede the ability of healthcare providers to provide effective care [8].

Emotional intelligence can help healthcare providers address these issues by enabling them to better understand and manage the emotional aspects of data sharing and privacy concerns. For example, healthcare providers with high levels of emotional intelligence can better understand patients' concerns around data sharing and privacy and can communicate more effectively with them to address their concerns. They can also work more effectively with other healthcare providers to ensure that patient data are shared securely and appropriately [9].

Overall, the healthcare providers must ensure that IoT devices are secure and patient data are protected by implementing various security measures such as encryption, authentication, access control, auditing, and privacy by design [10]. This will help to maintain patient trust and confidence in the use of IoT in healthcare. Data-sharing issues in healthcare systems with fusion-based approaches can be addressed by leveraging emotional intelligence to better understand and manage the emotional aspects of data sharing and privacy concerns. By doing so, healthcare providers can provide more effective care and improve patient outcomes, as shown in Figure 2.

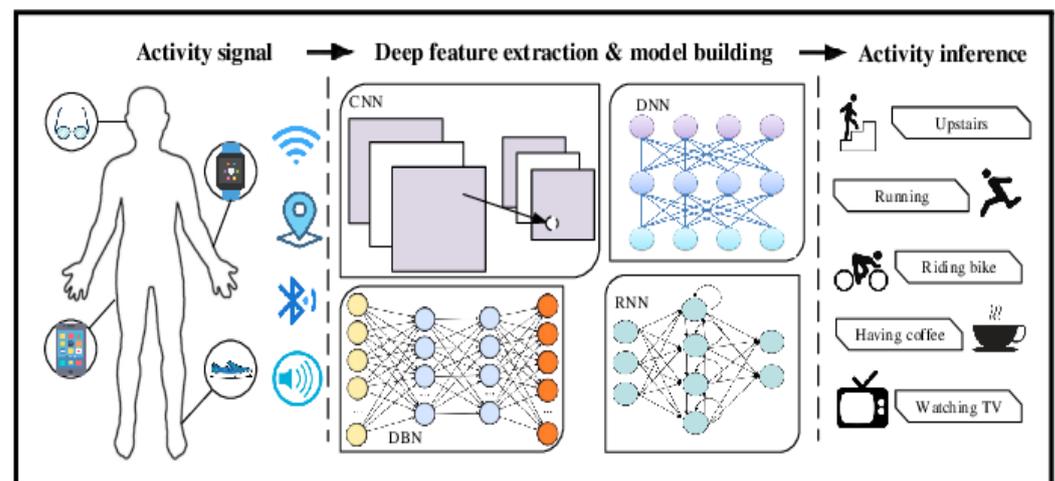


Figure 2. Artificial-intelligence-based IoT healthcare system.

The major demand for secure and efficient data-sharing solutions has prompted significant attention due to the increasing volume of shared sensor data. Leveraging a data fusion-based paradigm within the realm of IoT-protected healthcare systems has enabled the collection and analysis of patient data from diverse sources, encompassing medical devices, electronic health records (EHRs), and wearables. This innovative approach holds the potential to yield immediate benefits in terms of enhancing patient care, including more precise diagnoses and treatment plans. It empowers healthcare professionals to devise personalized treatment regimens by amalgamating data from multiple origins. Moreover, it has the capacity to alleviate financial burdens, elevate healthcare outcomes, and augment patient satisfaction. Furthermore, this concept extends to fortifying patient records against unauthorized access and potential misuse. In this study, we propose a novel approach for secure transmission of healthcare data, amalgamating the improved context-aware

data-fusion method with an emotional-intelligence-inspired enhanced dynamic Bayesian network (EDBN).

The remainder of this article's structure is as follows. Various background studies on the methods used for data security in the healthcare sector are included in Section 2. The suggested EDBN methodology for securing and categorizing IoT data for transmission is elaborated in Section 3. Results that validate performance and predictability are presented in Section 4 along with the appropriate explanations. In Section 5, the conclusion is presented along with future prospects.

2. Related Works and Background

2.1. Data Fusion for Healthcare Data Security in IoT

In recent years, there has been growing interest in using data-fusion techniques to enhance the security of healthcare data in the IoT. Data fusion can help detect anomalies and identify potential security threats by integrating data from enormous sources, such as electronic health records, wearables, and medical sensor devices.

Previous researchers [11–13] discussed a hybrid AI model that combines deep learning and fuzzy logic to analyze data from multiple IoT devices and optimize the network load. The article highlights the potential benefits of this approach for various applications, including healthcare, smart cities, and industrial automation. Another research group [14] presented a hybrid delay-aware adaptive clustering method for intelligent data fusion in wireless sensor networks. The method optimizes the data-fusion process by taking into consideration the communication delay and energy consumption of the sensor nodes. Refs [15,16] proposed an approach that uses a combination of rule-based and machine learning techniques to integrate data from multiple sources and generate meaningful insights. The study provided simulation findings that showed how the suggested strategy might enhance the precision and dependability of IoT health systems. Refs [17,18] proposed an Internet-of-Things (IoT)-enabled data-fusion method for sleep-healthcare applications that integrates data from multiple sources including wearable devices, smartphones, and environmental sensors. The proposed method uses a deep learning-based approach to extract features from the raw data and generate sleep-related metrics.

2.2. Healthcare with Emotional Intelligence in IoT

Studies [19–23] have discussed the potential of cognitive computing, emotional intelligence, and artificial intelligence in healthcare, with a focus on their applications in disease diagnosis, treatment, and personalized healthcare. Authors have suggested a disease-diagnostic paradigm for intelligent healthcare systems that is supported by artificial intelligence and the Internet of Things (IoT) and integrates data from multiple sources, including wearable devices, smartphones, and environmental sensors [24–32]. Researchers have provided an overview of the key concepts and technologies involved in AIoT healthcare architectures and highlighted the potential benefits of AIoT healthcare architectures, including improved patient care, reduced costs, and increased efficiency [33–42].

In summary, within the context of this review based on the above considerations in an IoT-based healthcare environment, a healthcare system with emotional intelligence within the IoT has the potential to improve patient outcomes, but there are several challenges that need to be addressed. These challenges include privacy and data-security concerns, integration with existing systems, reliability and accuracy of emotional intelligence analysis, user acceptance and adoption, ethical concerns, and the cost of IoT-based healthcare applications.

3. Materials and Methods

A. Low-Pass Filter

Low-pass filters are a type of filter that let low-frequency signals pass through while blocking or attenuating higher-frequency signals. In order to filter out noise and undesired high-frequency signals, low-pass filters are frequently employed in IoT healthcare data. This

can be especially important when dealing with patient data, as the noise and interference can be misinterpreted and lead to incorrect diagnoses or treatments.

$$H(s) = 1 / (1 + (s/\omega)^2) \quad (1)$$

where $H(s)$ is the transfer function of the filter, s is the frequency of the signal, and ω is the cutoff frequency of the filter.

$$(N = 1): Y(n) = (1/1) * X(n) = X(n) \quad (2)$$

$Y(n) = (1/N) * \sum X(k)$ is true for some arbitrary $N \geq 1$.

$$Y(n) = (1/(N+1)) * \sum X(k) = (1/(N+1)) * (X(n) + \sum X(k)) \quad (3)$$

A low-pass filter is a filter used to remove higher-frequency components from a signal. This type of filter is commonly used for preprocessing IoT healthcare data because it can reduce noise and other unwanted high-frequency components. Low-pass filters are also used to reduce the amount of high-frequency interference that can be present in a wireless signal. This is especially important when dealing with medical devices, as high-frequency interference can disrupt the signal and cause incorrect readings. Low-pass filters can help ensure that the signal remains clear and accurate, enabling more accurate readings and diagnoses.

$$Y(n) = X(n) * H(n) \quad (4)$$

where $Y(n)$ is the output signal, $X(n)$ is the input signal, $H(n)$ is the impulse response of the filter. A simple low-pass filter is a moving-average filter, which can be expressed as:

$$H(n)A = \frac{1}{N} * \sum_{k=0}^{N-1} X(n-k) \quad (5)$$

where N is the number of samples in the moving average.

The output signal can then be expressed as:

$$Y(n) = 1/N * \sum_{k=0}^{N-1} X(n-k) * X(n) \quad (6)$$

B. Improved Context-Aware Data Fusion (ICDF)

The improved context-aware data-fusion (ICDF) algorithm is an advanced data-fusion and analysis technique that combines multiple data sources and context information to create a single, comprehensive dataset. ICDF is particularly applicable to healthcare systems that involve both physical and virtual components and can be used to improve patient monitoring or medical decision making. In an IoT healthcare system, ICDF can be used to provide a better understanding of patient data by combining streaming real-time data from connected medical devices with patient-specific context information, such as age and medical history. By combining these different data sources, ICDF can provide more accurate and comprehensive patient information, which can be used to detect abnormalities, monitor patient conditions, and improve the accuracy of medical decision making. Algorithm 1 is shown the Improved context-aware data fusion (ICDF).

$$\text{Fused value} = P(x | \text{value1, value2, value3...Value N}) * P(x) \quad (7)$$

The ICDF algorithm also provides better scalability and flexibility for the healthcare system. By using multiple data sources and context information, the algorithm can be easily adapted to different scenarios and environments, making it suitable for large-scale healthcare systems. Additionally, the algorithm can be used to detect anomalies and trends in patient data, which can be used for further analysis and understanding of patient conditions.

A continuous-time signal is transformed mathematically into its frequency domain representation using the Fourier transform. It is described in terms of continuous data, and its formula is provided in Equations (8) and (9):

$$F(\omega) = \int [f(t) * \exp(-j\omega t)] dt \tag{8}$$

$$X[k] = \Sigma [x[n] * \exp(-j(2\pi/N) kn)] \tag{9}$$

Algorithm 1: Improved context-aware data fusion (ICDF)

- 1: **Input:** Set of sensor data S
 - 2: Step 1: Perform local data fusion to combine similar pieces of data into a single entity.
 - 3: Fused data = (Data1 + Data2 + Data3 + . . . + DataN)/N
 - 4: Step 2: For each entity in S, apply context-aware data-fusion methods to adjust the data based on context.
 - 5: Step 3: Aggregate the results of the individual data-fusion methods into a single entity using a weighted average or other suitable method.
 - 6: Step 4: Perform global data fusion on the aggregated entity using fuzzy logic or other suitable methods to adjust the data based on global context.
 - 7: **Output:** Single fused data entity.
-

Let $X = [x_1, x_2, \dots, x_n]$ be a set of n data sources, where x_i represents the data from the i-th source. Let $Y = [y_1, y_2, \dots, y_m]$ be a set of m contextual attributes, where y_i represents the contextual attribute from the i-th source.

Let $Z = [z_1, z_2, \dots, z_n]$ be the data-fusion result, where z_i represents the fused data from the i-th source. The ICDF algorithm computes the fused data as follows:

The Markov model fusion equation is:

$$Z = f(X,Y) = (1 - \alpha) * X + \alpha * Y \tag{10}$$

where α is the weighting factor for combining the fusion data Y with the observation data X, as mentioned in Equation (10).

Let us consider the exponential term, $\exp(-j\omega t)$. By Euler’s formula, we can express it as:

$$\exp(-j\omega t) = \cos(\omega t) - j * \sin(\omega t) \tag{11}$$

Substituting this back into the original equation, we have:

$$F(\omega) = \int [f(t) * (\cos(\omega t) - j * \sin(\omega t))] dt \tag{12}$$

We can separate the integral into two parts: one for the real part (cosine) and one for the imaginary part (sine). Let us start with the real part:

$$F(\omega) = \int [f(t) * \cos(\omega t)] dt$$

To evaluate this integral:

$$\int [f(t) * \cos(\omega t)] dt = (1/2) * \int [f(t) * (e^{j\omega t} + e^{-j\omega t})] dt \tag{13}$$

Now, we can expand the exponential terms:

$$F(\omega) = (1/2) * \int [f(t) * e^{j\omega t}] dt + (1/2) * \int [f(t) * e^{-j\omega t}] dt$$

Applying the linearity property of integrals, we can separate the integrals:

$$F(\omega) = (1/2) * \int [f(t) * e^{j\omega t}] dt + (1/2) * \int [f(t) * e^{-j\omega t}] dt$$

Since the function $f(t)$ is real-valued, the two integrals are complex conjugates of each other:

$$\begin{aligned} F(\omega) &= (1/2) * \int [f(t) * e^{j\omega t}] dt + (1/2) * \int [f(t) * e^{-j\omega t}] dt \\ F(\omega) &= (1/2) * \int [f(t) * e^{j\omega t}] dt + (1/2) * [\int [f(t) * e^{j\omega t}] dt]^* \end{aligned} \quad (14)$$

Simplifying, we have:

$$F(\omega) = (1/2) * \int [f(t) * e^{j\omega t}] dt + (1/2) * [\int [f(t) * e^{j\omega t}] dt]^* \quad (15)$$

$$F(\omega) = \int [f(t) * \exp(-j\omega t)] dt \quad (16)$$

Equation (12) states that the Fourier transform of a signal $f(t)$ is equal to the integral of the product of the signal $f(t)$ and the complex exponential $\exp(-j\omega t)$, where ω is the angular frequency. In the context of IoT healthcare data fusion, this equation can be used to analyze the frequency components of healthcare data from different sources. By performing the Fourier transform, one can analyze the frequency content of the data to identify patterns and correlations between different data sources.

Contextual attribute weighting: The first step of the ICDF algorithm is to weight the contextual attributes based on their importance in the current context.

Let $w = [w_1, w_2, \dots, w_m]$ be the weight vector for the contextual attributes, where w_i represents the weight for the i -th contextual attribute. The weight vector can be calculated using a variety of techniques, such as entropy-based weighting or principal component analysis.

Data normalization: The second step is to normalize the data from each source to ensure that they are on the same scale. This is done to prevent sources with larger values from dominating the fusion result. Let x_i' be the normalized data from the i -th source, which can be calculated as follows:

$$x_i' = \frac{(x_i - \min(x_i))}{(\max(x_i) - \min(x_i))} \quad (17)$$

where, in Equation (13), $\min(x_i)$ and $\max(x_i)$ represent, respectively, the minimum and maximum values of the data from the i -th source.

Contextual attribute-based data fusion: The third step is to fuse the normalized data based on the contextual attributes. Let $Z = [z_1, z_2, \dots, z_m]$ be the contextual attribute vector for the current context, where z_i represents the value of the i -th contextual attribute. The fused data d_i can be calculated as follows in Equation (14):

$$d_i = \frac{\sum_{j=1}^m (x_i' * w_j * \delta(z_i, y_j))}{\sum_{j=1}^m (w_j * \delta(z_i, y_j))} \quad (18)$$

where $x_i' * w_j$ is the normalized data from the i -th source for the j -th contextual attribute, $\delta(z_i, y_j)$ is the Kronecker delta function that returns 1 if $z_i = y_j$ and 0 otherwise, and $\sum_{j=1}^m (w_j * \delta(z_i, y_j))$ is the normalization factor.

C. Advanced Recursive Feature Elimination (ARFE)

Advanced recursive feature elimination (ERFE) is an advanced version of RFE that uses a genetic algorithm to search for the optimal feature set. ERFE works by iteratively removing attributes and building a model on those attributes that remain. It then evaluates the model. Note that ERFE is a computationally intensive algorithm and may require a

significant amount of time and resources to run on large datasets. Therefore, it is recommended to use ARFE with caution and consider other feature-selection algorithms if the computational cost is a concern.

Let X be the input dataset with n features and m samples, and y be the corresponding target variable. Let S be the initial set of candidate features, and k be the number of features to eliminate at each step. Let J be the performance metric to optimize.

Initialization: Set $S = \{x_1, x_2, \dots, x_n\}$, where x_i is the i -th feature in X . Train a machine learning model M_0 on the dataset using all the features in S . Compute the initial performance score $J_0 = J(y, M_0(X))$.

We can perform the features initialization with the given dataset:

$$y = (1/m)(x_1 * f_1 + x_2 * f_2 + \dots + x_m * f_m) - (1/m)(x_1 * y_1 + x_2 * y_2 + \dots + x_m * y_m) \quad (19)$$

Next, we can distribute $(1/m)$ to each term within the summations:

$$y = (1/m)x_1 * f_1 + (1/m)x_2 * f_2 + \dots + (1/m)x_m * f_m - (1/m)x_1 * y_1 - (1/m)x_2 * y_2 - \dots - (1/m)x_m * y_m$$

Now, we can rearrange the terms:

$$\begin{aligned} y &= [(1/m)x_1 * f_1 - (1/m)x_1 * y_1] + [(1/m)x_2 * f_2 - (1/m)x_2 * y_2] \dots + [(1/m)x_m * f_m \\ &\quad - (1/m)x_m * \dots * y_m] \\ y &= (1/m)[x_1 * (f_1 - y_1) + x_2 * (f_2 - y_2) + \dots + x_m * (f_m - y_m)] \\ y &= (1/m) \sum [x_i * (f_i - y_i)] \end{aligned} \quad (20)$$

Feature ranking: Compute the importance score of each feature in S , based on a ranking method such as correlation-based or filter-based methods.

Advanced Recursive feature elimination: Eliminate the k least important features from S , based on their importance scores. Let S' be the remaining features in S . Train a new machine learning model M_i on the dataset using the features in S' . Compute the performance score $J_i = J(y, M_i(X))$. If $J_i > J_{i-1}$, set $S = S'$ and go to step 2. If $J_i \leq J_{i-1}$, terminate the algorithm and select the features in S_{i-1} as the final feature subset.

This research uses a recursive approach to eliminate the least important features iteratively until the stopping criterion is met. The feature-selection process is based on the performance score of the machine learning model, and the feature-ranking method can be customized based on the specific problem domain. ARFE adds additional features to the basic RFE algorithm, such as dynamic programming and early stopping criteria, to improve the efficiency and accuracy of the feature-selection process.

$$\text{Feature Selection} = \left(\sum_{i=1}^n (X_i - \bar{X})^2 / (n - 1) \right) \quad (21)$$

where \bar{X} is the sample mean, X_i is a data point, and n is the number of data points.

Now, let us express the summation in terms of an integral. We assume a continuous probability distribution function $F(X)$ for the dataset.

The integral representation of the sample variance equation becomes:

$$\text{Feature Selection} = \int (X - \bar{X})^2 dF(X) = \int (X^2 - 2\bar{X}X + \bar{X}^2) dF(X).$$

Next, we can distribute the integral over each term:

$$\text{Feature Selection} = \int X^2 dF(X) - 2\bar{X} \int X dF(X) + \bar{X}^2 \int dF(X).$$

Now, let us simplify each integral term individually:

The first term, $\int X^2 dF(X)$, represents the expected value or the second moment of X , denoted as $E(X^2)$:

$$\text{Feature Selection} = E(X^2) - 2\bar{X}E(X) + \bar{X}^2 \int dF(X)$$

The second term, $\int X dF(X)$, represents the expected value or the first moment of X , denoted as $E(X)$:

$$\text{Feature Selection} = E(X^2) - 2\bar{X}E(X) + \bar{X}^2$$

Finally, the third term, $\int dF(X)$, represents the integral of the probability distribution function $F(X)$ over its entire range, which equals 1:

$$\text{Feature Selection} = E(X^2) - 2\bar{X}E(X) + \bar{X}^2$$

Therefore, the derived equation for feature selection using the integral representation is:

$$F(S) = E(X^2) - 2\bar{X}E(X) + \bar{X}^2 \tag{22}$$

This equation represents the feature-selection criterion based on the second moment ($E(X^2)$), the first moment ($E(X)$), the sample mean (\bar{X}) of the dataset, and $F(S)$ feature selection. The enhancement in this algorithm lies in calculating the average score improvement (ΔS) for each feature. It measures the impact of removing a feature on the model’s performance by considering the average improvement in the optimization criterion across multiple iterations. This helps in selecting features that consistently contribute the least to the overall performance.

D. Emotional-Intelligence-Based Healthcare System

Enhanced Dynamic Bayesian Network (EDBN)

A form of Bayesian network called a dynamic Bayesian network (DBN) is able to describe and analyze dynamic systems. These networks are used in a variety of applications, including healthcare systems. In particular, DBNs can be used to model the dynamics of patient healthcare and to identify potential interventions and outcomes. For example, a DBN can be used to identify the most appropriate treatments for a patient, based on their current health state and risk factors. It can also be used to predict the potential outcomes of a particular treatment or intervention. This can help healthcare providers make more informed decisions about treatments and interventions.

An EDBN can model different aspects of a patient’s health, including their medical condition, their lifestyle, and their environment. It can also represent the relationships between these factors and how they change over time. This allows healthcare providers to better understand and predict the progression of a patient’s health. EDBNs are composed of a set of nodes, each of which represents a random variable, and a set of directed edges that represent the conditional dependencies between the variables. These edges can be used to represent relationships between variables, such as how a patient’s symptoms can change over time.

The probability distribution equation for an enhanced Bayesian network is as follows:

$$P(M|N) = P(M \cap N) / P(N) \tag{23}$$

where M and N are two sets of random variables.

If we have variables $a_1, a_2, a_3 \dots a_n$, then the probabilities of a different combination of $a_1, a_2, a_3 \dots a_n$ are known as joint probability distribution.

$P[a_1, a_2, a_3, \dots, a_n]$ can be written in the following way in terms of the joint probability distribution:

$$\begin{aligned} &= P[a_1|a_2, a_3, \dots, a_n]P[a_2, a_3, \dots, a_n] \\ &= P[a_1|a_2, a_3, \dots, a_n]P[a_2|a_3, \dots, a_n] \dots P[a_{n-1}|a_n]P[a_n] \end{aligned}$$

In general, for each variable A_i , we can write the equation as:

$$P(A_i | A_i - 1, \dots, A_1) = P(A_i | \text{Parent}(A_i)) \tag{24}$$

EDBNs also incorporate temporal information, which allows them to incorporate changes in the system as time progresses. This makes them well suited for modeling healthcare data, as the dynamics of a patient’s health can change quickly over time. EDBNs are also used to model the relationships between variables in time-series data. This can be used to identify patterns in the data that may be useful for diagnosis or treatment. The proposed architecture of this research, in Figure 3, above, indicates the various data sources, such as data collected via smart phones, smart watches, hospitals, and others. These data are given to the neural network and the useful features are extracted, such as heart rate, blood pressure, and facial features such as eyes and mouth to identify the emotions of the patients. Here, the extracted features such as data for the eyes and mouth are converted into vectors and the vectors are added to the data obtained through sensor integration and given as input to the convolutional neural network, which helps in identification of the emotions of the person under various health conditions and vice versa. Here, the backpropagation algorithm with IDBN is used. The data fusion and the secure communications are achieved using the ICDF algorithm, ARFE, and IDBN network.

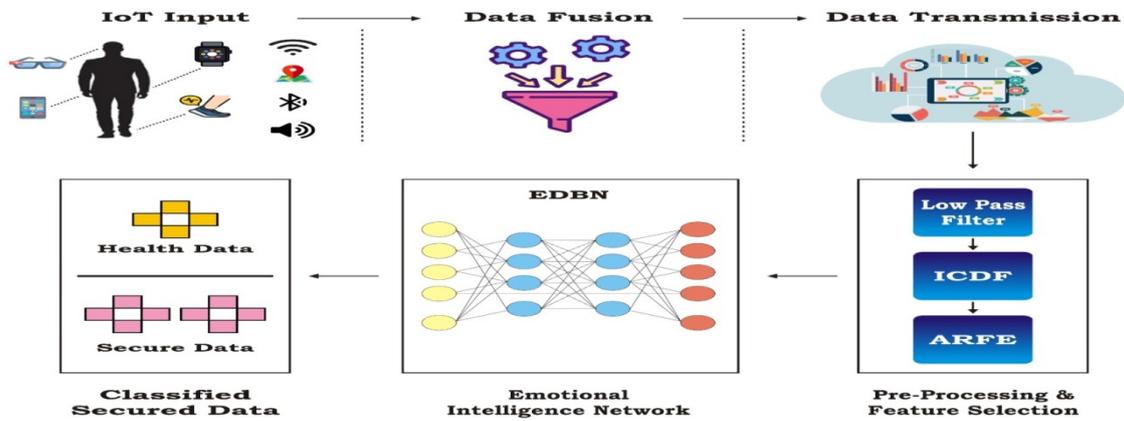


Figure 3. Proposed emotional-intelligence healthcare system.

4. Results and Discussion

With the use of two separate sets of databases for patients with ages ranging from 25 to 60, the findings of this study were examined. The dataset was first gathered to look at how sensor displacement affected activity recognition in actual environments. It expands on the ideas of self-placement, induced displacement, and optimal placement. As versions of extreme displacement, the ideal and mutual-displacement conditions might serve as boundary conditions for recognition algorithms. The dataset included a sizable number of people, sensor modalities, and extracted physical activities. It monitored 17 different participants as they engaged in 33 various behaviors, such as walking, running, jogging, leaping up, and jumping rope.

Precision

The precision of each model’s class predictions was measured. The calculation was performed by dividing the total number of true positives (TP) by the total number of true positives and false positives.

$$(FP) \cdot \text{Precision} = TP / (TP + FP) \tag{25}$$

Recall

Recall was computed by dividing the total number of true positives by the sum of true positives and false negatives.

$$\text{Recall} = TP / (TP + FN) \tag{26}$$

Accuracy

Accuracy is a measure of how accurately a model classifies all instances. It was calculated by dividing the number of true positives plus true negatives (TN) by the total number of instances.

$$\text{Accuracy} = (\text{TP} + \text{TN}) / (\text{TP} + \text{TN} + \text{FP} + \text{FN}) \quad (27)$$

F1 Score

The model's performance was evaluated using the F1 score, which combines precision and accuracy. The harmonic mean of precision and accuracy was used for its computation. The F-measure formula is as follows:

$$\text{F1 Score} = 2 * (\text{precision} * \text{accuracy}) / (\text{precision} + \text{accuracy}) \quad (28)$$

In Table 1, Figure 4, it is possible to see the F1 score, accuracy, precision, recall, and ROC-AUC score of the proposed methodology (EI-EDBN), as well as comparative results using a CNN, DCNN, and FRCNN. The F1 score, accuracy, precision, recall, and ROC-AUC score of the proposed method are 92.1%, 97.3%, 95.4%, 96.3%, and 0.52, respectively. It is possible to see that the EI-EDBN method leads to better outcomes.

Table 1. Performance Metrics Analysis.

Algorithms	Performance Metrics				
	Recall	Precision	Accuracy	F1 Score	ROC-AUC Score
CNN	73.2	78.4	84.3	75.1	0.73
DCNN	92.1	91.4	87.4	89.3	0.56
FRCNN	85.3	89.1	83.2	81.5	0.61
Proposed EI-EDBN	96.3	95.4	97.3	92.1	0.52

In addition, F1 score, accuracy, precision, recall, and ROC-AUC score using DCNN were found to be 89.3%, 87.4%, 91.4%, 92.1%, and 0.56, respectively, which were second-highest to the proposed method. On the other hand, the F1 scores, accuracy, precision, recall, and ROC-AUC scores of FRCNN and CNN were low in accuracy, at 83.2% and 84.3%, respectively.

Figure 5a–d display the results of the performance comparison for datasets I and II. The graph clearly illustrates how the performances of the suggested and existing tactics compare. Figure 4a displays the outcomes of the recommended EI-EDBN's recall comparison for healthcare data, and it can also be observed from the data that the recommended EI-EDBN technique yielded extremely exact results. Figure 4b displays the outcome of precision comparisons using the proposed EI-EDBN model for healthcare data. It can be noted from the results that the recommended EI-EDBN technique has excellent recall performance. Figure 4c displays the accuracy comparison of the proposed EI-EDBN model for healthcare data. So, it is concluded that EI-EDBN is the recommended strategy.

In Figure 5, the results of the performance comparison for the two datasets are displayed. The results demonstrate that the suggested approach outperformed the conventional approaches for both datasets.

Table 2 displays the performance comparison results for the two datasets. We infer from Table 2 that the performance results of the proposed approach are better for dataset 1 than for dataset 2. Figure 5a,b display the outcomes of the comparison of recall and precision for the two datasets. Additionally, it is clearly shown that the recommended technique produces superior results than the ones being used now. Figure 5c,d display the comparison of accuracy and F1 score for both datasets.

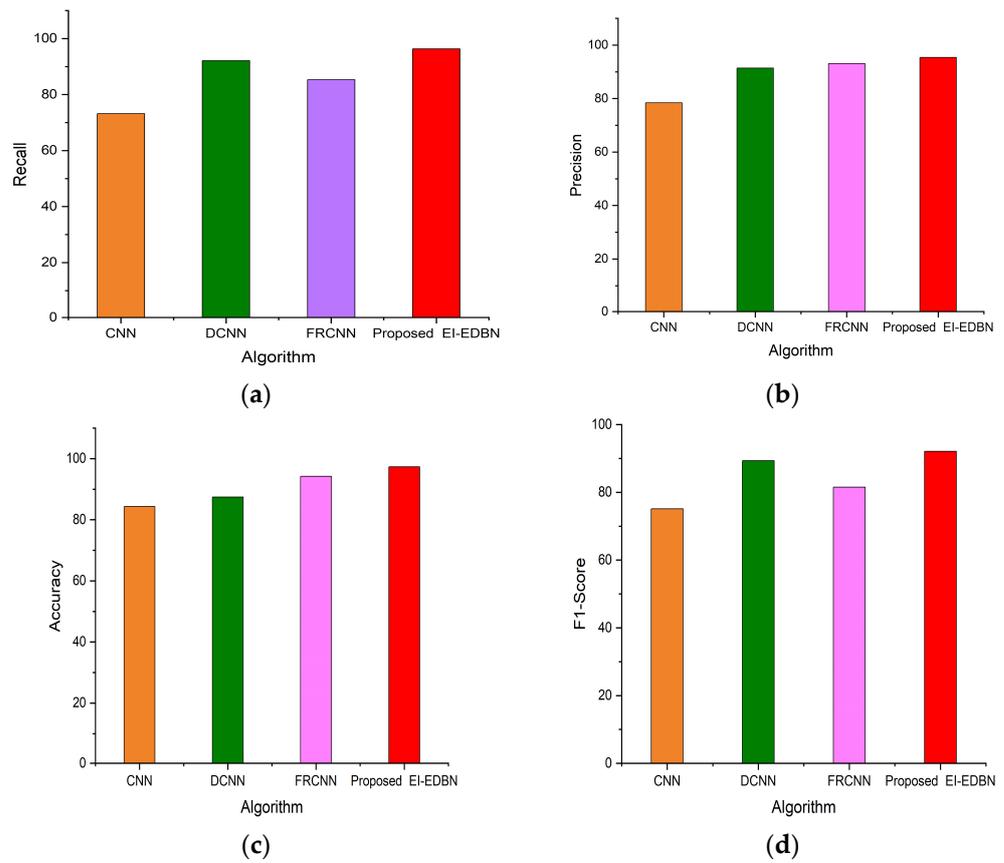


Figure 4. (a) Comparison of recall; (b) comparison of precision; (c) comparison of accuracy; (d) comparison of F1 score.

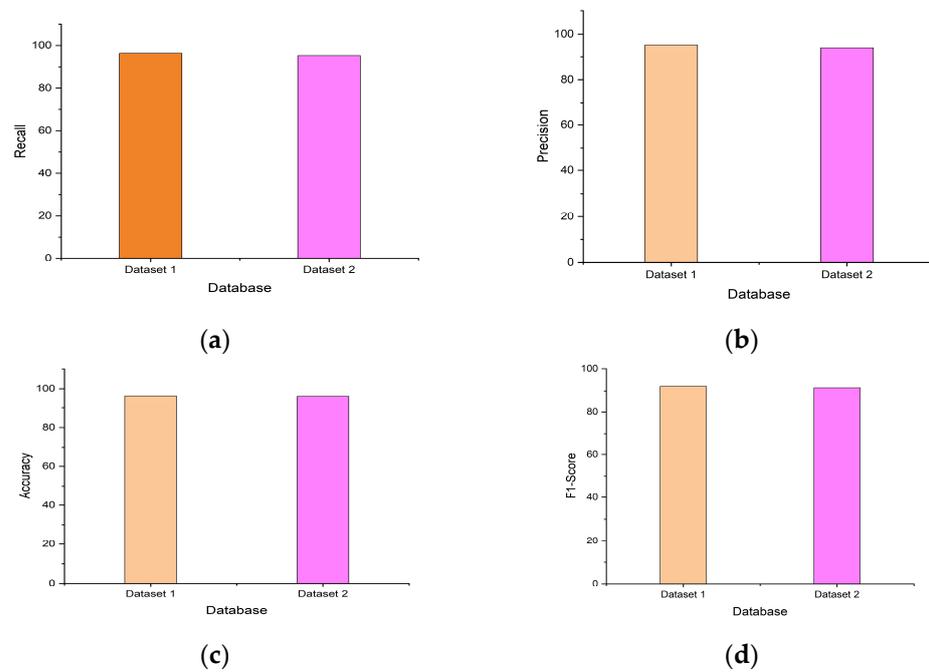


Figure 5. (a) Comparison of datasets for recall; (b) comparison of datasets for precision; (c) comparison of datasets for accuracy; (d) comparison of datasets for F1 score.

Table 2. Performance Comparison Results.

DATABASE	Performance Metrics			
	Recall	Precision	Accuracy	F1 Score
DATASET 1	96.3	95.4	96.3	92.1
DATASET 2	95.3	94.2	96.1	91.4

5. Conclusions

Fusion-based secure healthcare with emotional-intelligence integration for sharing sensor data and the IoT is a promising approach to improving the monitoring of patient health by fusing data from various sources, including sensors and IoT devices, analyzing the data using machine learning algorithms, and detecting emotions to provide a holistic view of patient health. The merging of data from numerous sources enables healthcare practitioners to monitor patients' health in real time, identify possible health risks, and deliver prompt treatments. The use of emotional intelligence enables physicians to recognize emotional states that may have an influence on patient health and give necessary care. Secure communication is essential for maintaining the security, integrity, and availability of patient data. The EI-EDBN technique proposed in this research ensures the secured communication protocols are included in the encrypted data in transit and ensures that only authorized individuals may access the data. Also, the emotional-intelligence-trained model of this system classifies all the relevant health data from the group of patients, which makes it easier for the information provider to treat the data accurately and securely. Overall, fusion-based secure healthcare with emotional-intelligence integration for sensor data sharing and the IoT has the potential to revolutionize monitoring of patient health and improve healthcare outcomes by providing a comprehensive view of patient health, early detection of potential health issues, and timely interventions. As IoT devices and sensors are increasingly utilized in the healthcare field, this approach holds immense potential for various future applications, such as enhancing remote patient monitoring, facilitating personalized medicine, and managing population health. Moreover, this approach can be effectively applied to other areas of healthcare, such as monitoring mental health and managing chronic diseases. Furthermore, integrating emotional intelligence into healthcare can greatly impact patient satisfaction and overall quality of care. With ongoing technological advancements, there is also the potential for this approach to incorporate more sophisticated machine learning algorithms and data-analysis techniques, thereby providing more precise and individualized insights. By collaborating with industry partners and healthcare organizations, practical implementation strategies for this approach can be developed for real-world healthcare settings. In summary, the possibilities for this work are vast and have the potential to significantly enhance healthcare delivery and improve patient outcomes.

Author Contributions: Conceptualization, M.A.A.; Methodology, S.Y., M.A.A., L.A., N.K.B.C., K.K., P.V., F.H. and T.A.; Software, M.A.A. and S.Y.; Validation, S.Y., M.A.A., L.A., N.K.B.C., K.K., P.V., F.H. and T.A.; Formal analysis, S.Y., M.A.A., L.A., N.K.B.C., K.K., P.V., F.H. and T.A.; Investigation, S.Y., M.A.A., L.A., N.K.B.C., K.K., P.V., F.H. and T.A.; Data curation, S.Y., M.A.A., L.A., N.K.B.C., K.K., P.V., F.H. and T.A.; Writing—original draft, L.A.; Writing—review & editing, S.Y., M.A.A., L.A., N.K.B.C., K.K., P.V., F.H. and T.A. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Project No. Grant No. 4446) and Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R236), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Institutional Review Board Statement: Not applicable in this research.

Informed Consent Statement: Not applicable for this research.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ji, G.; Msigwa, C.; Bernard, D.; Lee, G.; Woo, J.; Yun, J. Health24: Health-related Data Collection from Wearable and Mobile Devices in Everyday Lives. In Proceedings of the 2023 IEEE International Conference on Big Data and Smart Computing (BigComp), Jeju, Republic of Korea, 13–16 February 2023; pp. 336–337.
2. Chen, J.; Song, X.; Huang, Z.; Li, J.; Wang, Z.; Luo, C.; Yu, F. On-Site Colonoscopy Autodiagnosis Using Smart Internet of Medical Things. *IEEE Internet Things J.* **2021**, *9*, 8657–8668. [[CrossRef](#)]
3. Jain, D.K.; Boyapati, P.; Venkatesh, J.; Prakash, M. An intelligent cognitive-inspired computing with big data analytics framework for sentiment analysis and classification. *Inf. Process. Manag.* **2022**, *59*, 102758. [[CrossRef](#)]
4. Ezhilarasi, M.; Kumar, A.; Shanmugapriya, M.; Ghanshala, A.; Gupta, A. Integrated Healthcare Monitoring System using Wireless Body Area Networks and Internet of Things. In Proceedings of the 2023 4th International Conference on Innovative Trends in Information Technology (ICITIT), Kottayam, India, 11–12 February 2023; pp. 1–5.
5. Shrivastava, K.; Kumar, S.; Jain, D.K. An effective approach for emotion detection in multimedia text data using sequence based convolutional neural network. *Multimed. Tools Appl.* **2019**, *78*, 29607–29639. [[CrossRef](#)]
6. Xu, G.; Qi, C.; Dong, W.; Gong, L.; Liu, S.; Chen, S.; Liu, J.; Zheng, X. A Privacy-Preserving Medical Data Sharing Scheme Based on Blockchain. *IEEE J. Biomed. Health Inform.* **2022**, *27*, 698–709. [[CrossRef](#)] [[PubMed](#)]
7. Saranya, S.S.; Fatima, N.S. IoT-Based Patient Health Data Using Improved Context-Aware Data Fusion and Enhanced Recursive Feature Elimination Model. *IEEE Access* **2022**, *10*, 128318–128335. [[CrossRef](#)]
8. Jin, H.; Luo, Y.; Li, P.; Mathew, J. A Review of Secure and Privacy-Preserving Medical Data Sharing. *IEEE Access* **2019**, *7*, 61656–61669. [[CrossRef](#)]
9. Perez, S.; Hernandez-Ramos, J.L.; Pedone, D.; Rotondi, D.; Straniero, L.; Skarmeta, A.F. A Digital Envelope Approach Using Attribute-Based Encryption for Secure Data Exchange in IoT Scenarios. In Proceedings of the Global Internet of Things Summit, Geneva, Switzerland, 6–9 June 2017; pp. 1–6. [[CrossRef](#)]
10. Wang, J.; Chen, Y.; Hao, S.; Peng, X.; Hu, L. Deep learning for sensor-based activity recognition: A survey. *Pattern Recognit. Lett.* **2019**, *119*, 3–11. [[CrossRef](#)]
11. Mukherjee, A.; Jain, D.K.; Yang, L. On-demand efficient clustering for next generation IoT applications: A hybrid NN approach. *IEEE Sens. J.* **2020**, *21*, 25457–25464. [[CrossRef](#)]
12. Theodouli, A.; Arakliotis, S.; Moschou, K.; Votis, K.; Tzovaras, D. On the Design of a Blockchain-Based System to Facilitate Healthcare Data Sharing. In Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering, New York, NY, USA, 31 July–3 August 2018; pp. 1374–1379. [[CrossRef](#)]
13. Jan, M.A.; Zakarya, M.; Khan, M.; Mastorakis, S.; Menon, V.G.; Balasubramanian, V.; Rehman, A.U. An AI-enabled lightweight data fusion and load optimization approach for Internet of Things. *Future Gener. Comput. Syst.* **2021**, *122*, 40–51. [[CrossRef](#)]
14. Liu, X.; Zhu, R.; Anjum, A.; Wang, J.; Zhang, H.; Ma, M. Intelligent data fusion algorithm based on hybrid delay-aware adaptive clustering in wireless sensor networks. *Future Gener. Comput. Syst.* **2020**, *104*, 1–14. [[CrossRef](#)]
15. Devika, E.; Saravanan, A. Enhanced gray wolf optimization for estimation of time difference of arrival in WSNs. *Int. J. Pervasive Comput. Commun.* **2022**; ahead-of-print. [[CrossRef](#)]
16. Devika, E.; Saravanan, A. A survey of node localization in wireless sensor networks using various Optimization algorithms. In Proceedings of the 2022 Third International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), Bengaluru, India, 16–17 December 2022; pp. 1–8. [[CrossRef](#)]
17. Kandasamy, M.; Anto, S.; Baranitharan, K.; Rastogi, R.; Satwik, G.; Sampathkumar, A. Smart Grid Security Based on Blockchain with Industrial Fault Detection Using Wireless Sensor Network and Deep Learning Techniques. *J. Sens.* **2023**, *2023*, 3806121. [[CrossRef](#)]
18. Arumugam, S.; Shandilya, S.K.; Bacanin, N. Federated Learning-Based Privacy Preservation with Blockchain Assistance in IoT 5G Heterogeneous Networks. *J. Web Eng.* **2022**, *21*, 1323–1346. [[CrossRef](#)]
19. Baloch, Z.; Shaikh, F.K.; Unar, M.A. A context-aware data fusion approach for health-IoT. *Int. J. Inf. Technol.* **2018**, *10*, 241–245. [[CrossRef](#)]
20. Yang, F.; Wu, Q.; Hu, X.; Ye, J.; Yang, Y.; Rao, H.; Hu, B. Internet-of-Things-enabled data fusion method for sleep healthcare applications. *IEEE Internet Things J.* **2021**, *8*, 15892–15905. [[CrossRef](#)]
21. Alloghani, M.; Al-Jumeily, D.; Mustafina, J.; Hussain, A.; Aljaaf, A.J. A systematic review on supervised and unsupervised machine learning algorithms for data science. In *Supervised and Unsupervised Learning for Data Science*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 3–21.
22. Satamraju, K.P.; Balakrishnan, M. A secured healthcare model for sensor data sharing with integrated emotional intelligence. *IEEE Sens. J.* **2022**, *22*, 16306–16313. [[CrossRef](#)]
23. Mansour, R.F.; El Amraoui, A.; Nouaouri, I.; Díaz, V.G.; Gupta, D.; Kumar, S. Artificial intelligence and internet of things enabled disease diagnosis model for smart healthcare systems. *IEEE Access* **2021**, *9*, 45137–45146. [[CrossRef](#)]
24. Pise, A.A.; Almusaini, K.K.; Ahanger, T.A.; Farouk, A.; Pareek, P.K.; Nuagah, S.J. Enabling artificial intelligence of things (aiot) healthcare architectures and listing security issues. *Comput. Intell. Neurosci.* **2022**, *2022*, 8421434. [[CrossRef](#)] [[PubMed](#)]
25. Almaiah, M.A.; Ali, A.; Hajje, F.; Pasha, M.F.; Alohal, M.A. A lightweight hybrid deep learning privacy preserving model for FC-based industrial internet of medical things. *Sensors* **2022**, *22*, 2112. [[CrossRef](#)] [[PubMed](#)]

26. Hatzivasilis, G.; Soultatos, O.; Ioannidis, S.; Verikoukis, C.; Demetriou, G.; Tsatsoulis, C. Review of security and privacy for the Internet of Medical Things (IoMT). In Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini, Greece, 29 May 2019; pp. 457–464.
27. Papaioannou, M.; Karageorgou, M.; Mantas, G.; Sucasas, V.; Essop, I.; Rodriguez, J.; Lymberopoulos, D. A survey on security threats and countermeasures in internet of medical things (IoMT). *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4049. [[CrossRef](#)]
28. Almaiah, M.A. A new scheme for detecting malicious attacks in wireless sensor networks based on blockchain technology. In *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*; Springer International Publishing: Cham, Switzerland, 2021; pp. 217–234.
29. Alamer, M.; Almaiah, M.A. Cybersecurity in Smart City: A systematic mapping study. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 719–724.
30. Manickam, P.; Mariappan, S.A.; Murugesan, S.M.; Hansda, S.; Kaushik, A.; Shinde, R.; Thipperudraswamy, S.P. Artificial intelligence (AI) and internet of medical things (IoMT) assisted biomedical systems for intelligent healthcare. *Biosensors* **2022**, *12*, 562. [[CrossRef](#)]
31. Razdan, S.; Sharma, S. Internet of medical things (IoMT): Overview, emerging technologies, and case studies. *IETE Tech. Rev.* **2022**, *39*, 775–788. [[CrossRef](#)]
32. Altulaihah, E.; Almaiah, M.A.; Aljughaiman, A. Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions. *Electronics* **2022**, *11*, 3330. [[CrossRef](#)]
33. Albalawi, A.M.; Almaiah, M.A. Assessing and reviewing of cyber-security threats, attacks, mitigation techniques in IoT environment. *J. Theor. Appl. Inf. Technol.* **2022**, *100*, 2988–3011.
34. Joyia, G.J.; Liaqat, R.M.; Farooq, A.; Rehman, S. Internet of medical things (IoMT): Applications, benefits and future challenges in healthcare domain. *J. Commun.* **2017**, *12*, 240–247.
35. AlSalem, T.S.; Almaiah, M.A.; Lutfi, A. Cybersecurity Risk Analysis in the IoT: A Systematic Review. *Electronics* **2023**, *12*, 3958. [[CrossRef](#)]
36. Almaiah, M.A. An Efficient Smart Weighted and Neighborhood-enabled Load Balancing Scheme for Constraint Oriented Networks. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*, 1–11. [[CrossRef](#)]
37. Gautam, D.; Dixit, A.; Goyal, S.B.; Verma, C.; Kumar, M. A novel approach to enhance the quality of health care recommender system using fuzzy-genetic approach. *J. Intell. Fuzzy Syst.* **2023**, 1–4, preprint.
38. Ghubaish, A.; Salman, T.; Zolanvari, M.; Unal, D.; Al-Ali, A.; Jain, R. Recent advances in the internet-of-medical-things (IoMT) systems security. *IEEE Internet Things J.* **2020**, *8*, 8707–8718. [[CrossRef](#)]
39. Javaheri, D.; Lalbakhsh, P.; Hosseinzadeh, M. A novel method for detecting future generations of targeted and metamorphic malware based on genetic algorithm. *IEEE Access* **2021**, *9*, 69951–69970. [[CrossRef](#)]
40. Alsayouf, A.; Lutfi, A.; Al-Bsheish, M.; Jarrar, M.T.; Al-Mugheed, K.; Almaiah, M.A.; Alhazmi, F.N.; Masa’deh, R.E.; Anshasi, R.J.; Ashour, A. Exposure detection applications acceptance: The case of COVID-19. *Int. J. Environ. Res. Public Health* **2022**, *19*, 7307. [[CrossRef](#)]
41. Vishnu, S.; Ramson, S.J.; Jegan, R. Internet of medical things (IoMT)-An overview. In Proceedings of the 2020 5th International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India, 5–6 March 2020; pp. 101–104.
42. Mishra, K.N.; Chakraborty, C. A novel approach towards using big data and IoT for improving the efficiency of m-health systems. In *Advanced Computational Intelligence Techniques for Virtual Reality in Healthcare*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 123–139.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.