SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I10P112

Volume 12 Issue 10, 129-146, October 2025

Original Article

Rule-Based Cyber Security Model with Adaptive Interval Type-2 Fuzzy Neural Networks in Multi-Sensor Data Monitoring

Radhika Rajoju[1], P. Swetha[2]

[1,2]*JNTUH, Department of CSE, Hyderabad, Telangana, India.*

[1]*Corresponding Author : radhika.rajoju2020@gmail.com*

Received: 12 August 2025 Revised: 14 September 2025 Accepted: 13 October 2025 Published: 31 October 2025

Abstract - *In the context of multi-sensor data monitoring systems, especially in critical domains like Healthcare, cybersecurity plays a pivotal role in ensuring the integrity, confidentiality, and availability of the data being collected, transmitted, and analyzed. These systems often gather sensitive physiological and behavioral information from multiple sensors—such as ECG, EEG, temperature, blood pressure, and movement sensors-making them prime targets for cyberattacks. Unauthorized access or tampering with this data can lead to serious consequences, including incorrect diagnoses, compromised patient safety, and data privacy breaches. In this paper, a Rule-Based Adaptive Type-2 Fuzzy Neural Network (RbAFNN) and an HMM are used to manage data from multiple sensors in healthcare monitoring. With interval Type-2 fuzzy logic and the adaptive neural network, the approach can properly work with uncertain and imprecise data and quickly self-adjust to new changes in patients. With HMM, sensor data are handled properly over time, so fault detection and health classification improve. Experiments with several healthcare-related datasets find that the RbAFNN-HMM model delivers high accuracy, a high sensitivity level, and a low number of false positives in the tasks of health monitoring and cyber threat detection with efficient performance in real-time. Experimental analysis stated that the accuracy of detecting a phone call with the RbAFNN-HMM model is more than 96%, it has a 97% sensitivity, and its false positives are no more than 3%. The system is very accurate in detecting threats, as its threat detection is around 92% for different attack types, and it usually mitigates threats with a success rate above 89%. These results prove that the framework helps deliver correct, prompt, and secure health care, thereby making it a dependable solution for changing and uncertain situations in hospitals. The framework's solid cybersecurity features ensure that important data is safe and better protected against DoS, spoofing, and data injection. The advanced solution offered by the system is reliable, smart, and ensures security in unstable and uncertain situations.*

Keywords - *Healthcare Monitoring, Cybersecurity, Multi-Sensor, Type-2 Fuzzy, Hidden Markov Model (HMM), Neural Network, Rule-Based Model.*

1. Introduction

Recently, using multiple sensors together has played a crucial role in health monitoring because it offers more accurate, dependable, and broader information about patients' health [1]. With individual ECG, accelerometers, temperature sensors, and blood oxygen monitors, data from which multi-sensor fusion techniques make it possible to eliminate issues associated with each individual sensor, for example, noise, drift, or data missing [2]. Using machine learning and signal processing, new technologies are now able to provide more valuable information about someone's health by intelligently analyzing various data. Therefore, illnesses are more easily identified in the early stages, issues are recognized immediately, and monitoring for each individual is improved [3]. Setting up remote patient monitoring, smart wearable tech, and Healthcare for the elderly, as well as rehabilitation, have all made Healthcare more involved in inpatient care. Since data collected by sensors is sometimes not the same, using them together becomes a real challenge. Matching data from various sources is hard, particularly in real-time cases, because any disruption or lag can cause wrong conclusions to be drawn [4, 5]. Also, if sensors are not dependable or if there is a lot of noise from them, the data may not be accurate, and using the data could impair the system's performance [6]. More concerns about privacy and security exist now because a lot of private health data is being collected and exchanged. Handling huge, ongoing flows of multi-form data can be difficult because this task needs plenty of resources and efficient algorithms. Standardization of how sensors communicate and share data is still lacking, which makes it

difficult for various healthcare settings to use these technologies together [7 -10].

Nevertheless, a number of challenges still exist. Information observed through various sensors is typically heterogeneous, and the combination of readings in real time is challenging because of mismatch, latency, and unreliability of the sensors that may result in erroneous inferences. The notion of privacy and information security is augmented since sensitive health information is perpetually captured, relayed, and distributed. Processing huge and constant flows of multimodal data requires significant computing power and algorithms, but the sensor communication has not been standardized yet, restricting the interoperability of healthcare facilities. The issue of security in multi-sensor data fusion is essential since the presence of a compromised sensor may threaten medical decision reliability. Though novel approaches, such as blockchain, federated learning, role-based access control, and running frequent updates to the firmware ensure a higher level of data security, combining them without lowering real-time capabilities is still a challenge, especially when operating on wearable or edge devices with limited resources. Additionally, whereas CNNs, RNNs, and transformers show a benefit when applied to the automatic processing of nonlinear and noisy sensor data, the literature is mostly restricted to a particular type of sensors or sound, noise-free sensor inputs, and knowledge about fusion frameworks that can be easily and securely applied to healthcare applications in a real-time setting remains scarce. The world urgently needs infrastructure that would support heterogeneous sensor data, cybersecurity, real-time efficiency on edge devices, and high-fidelity and personalized healthcare information. This paper will discuss these challenges by providing a Multi-sensor fusion framework based on deep learning that would help overcome the pitfalls of uncertainty, dynamic patient conditions, and cyber-threats in healthcare monitoring.

Security in data fusion plays a vital role, especially in Healthcare, as patient information is always being gathered, shared, and used [11, 12]. Since multi-sensor setups need to share data over the network, they face several types of cyber threats, such as people stealing data, breaking into networks, imitating legitimate people, and changing information [13-15]. The data should always be secured by advanced measures like encryption, proper communication methods, user authentication, and quick detection of threats. As well, the process used to combine all the data should be kept safe from change, as one affected sensor could spoil the entire analysis and provide wrong medical support [16, 17]. The issue becomes more difficult due to the limited resources on wearable and edge devices that can handle complex security algorithms. As a result, making cybersecurity solutions light and flexible for multi-sensor fusion systems is crucial to keep trust, guard patient privacy, and depend on healthcare monitoring tools. Recent work has tried to embed these cybersecurity measures straight into the design of multi-sensor healthcare systems [18]. Blockchain, machine learning, and federated learning are means for keeping data safe and reliable. Both role-based access controls and regular firmware security updates work to stop any security threats that may strain the network. At the same time, making sure the system is secure without it slowing down too much is still a major issue in real-time medicine, since any delay can harm patients [19]. Compliance with regulations like HIPAA and GDPR is important, and it stresses the requirement for stronger cybersecurity plans. In Healthcare, securing effective multi-sensor data fusion alongside the increased use of new technologies is needed to build trust with patients and ensure the future of AI-driven medical solutions [20].

Deep learning in multi-sensor healthcare systems is improved because it helps with automatically analyzing data, identifying complicated signals, and making precise decisions. In contrast to regular machine learning methods, deep learning models, for example, CNNs, RNNs, and transformers, are able to learn from raw data collected by various sensors [21]. Using this approach is especially helpful in Healthcare since sensor measurements are usually messy, complicated to process, and related to changes over time. The combination of several sources of data, enabled by deep learning, helps analyze a patient's situation more deeply and in full detail. Some uses are forecasting diseases, finding unusual patterns, noticing activities, and offering personalized care suggestions [22].

With edge AI, deep learning models can now be used on wearable devices to do processing right away and make fewer connections to cloud servers [23-26]. The paper contributes a lot to healthcare monitoring by solving the problems of uncertainty, shifting patient statuses, and cyber crimes related to multi-sensor information. The key aim is to design a solid system that can notice any health concerns in real-time and keep health records safe from potential cyber threats. Thus, the paper suggests implementing a Rule-Based Adaptive Interval Type-2 Fuzzy Neural Network (RbAFNN) along with a Hidden Markov Model (HMM). With help from interval Type-2 fuzzy logic, a neural network, and HMM, this approach correctly classifies a person's health status by considering sensor data fluctuations and their patterns over time. Lots of experiments were carried out using data such as PhysioNet, MIMIC-III, and fabricated sensor information, showing that the approach achieved a detection accuracy of 96.5%, as high as a sensitivity of 97.0% and a false positive rate as low as 3.2%. When being evaluated, the model notices many types of attacks and deals with them effectively, with accuracy rates higher than 92% and success in mitigation reaching above 89%, all the while responding in under 22 milliseconds. The findings confirm that the model is accurate, prompt, and secure, which makes it suitable for practical use in real hospitals.

2. Related Works

Over the years, there has been a strong increase in Healthcare, with intelligent systems being used to monitor patients through various sensors. Because there is now more and more sensor-generated data, making sure it remains secure and uncompromised is becoming urgent. Old methods of cybersecurity are usually not effective enough for the changing and unpredictable nature of medical data. In this situation, adding decision-making capabilities to existing cybersecurity rules can produce satisfying results. This related works section studies how a Rule-Based Cybersecurity Model using Adaptive Interval-Type-2 Fuzzy Neural Networks (IT2FNNs) can be used in multi-sensor environments. This model uses rule-based understanding and the flexible and uncertain approach of fuzzy neural networks to provide a stronger and smarter defense from cyber threats in healthcare monitoring. It brings out key points about the development, issues, and achievements of other models on which the new method can be based.

Lee (2023) covers the use of intelligent control theory in process enhancement and manufacturing, giving the key background needed to use such methods in Healthcare. They note that a smart combination of machine learning with multi-sensor data helps drone systems spot risks in real time. In 2025, Xin and his co-authors propose a way to handle secure state estimation in cyber-physical systems, using virtual sensors and deep reinforcement learning, suggesting it may successfully manage coordinated sensor attacks. Potamos et al. discuss the role of various sensor data in maritime cybersecurity and stress that fusing them helps make monitoring more effective. Daş and Tuna (2025) also discuss the benefits of data fusion in smart grid analytics, by stressing that fusion models are essential for running complicated data-managed systems. All these experiments demonstrate the importance of using adaptive, intelligent, and reliable data fusion frameworks, such as those generated by fuzzy neural networks, in systems that monitor threats using various sensors.

Kong and Yang (2024) present a system that can estimate train speed and position even when faced with attacks or physical problems, proving the need for protection in important systems. Szynkiewicz et al. (2023) look into how deep learning is applied to the cybersecurity of robotic systems, and their research shows that deep learning is useful for recognizing different data patterns from sensors. Hu et al. (2024) put together a multi-sensor fusion system for laboratory monitoring and proved how it can secure critical environments. Hua and Hao (2023) also look at fusion and detection in systems under false data injection attacks, stressing how to prevent problems caused by interference. The researchers from Liu et al. (2024) contribute to safe and protected IoT-based sensor systems by introducing an approach based on adaptive privacy budgets. In their work, Desikan et al. use both machine learning and other technologies to help sensors work under conditions of fault tolerance, thereby assisting with mitigating fire risks. Their study (Cheng et al.) explores how decentralized consensus can still be used under threats and missing data. In 2024, Li and Supriya demonstrate the use of intelligent monitoring and control systems that rely on data from several sensors to help detect anomalies and forecast faults, demonstrating different areas of usefulness.

Li and Qiang (2023) offer an adaptive Kalman filter for better data fusion, and Hallyburton et al. (2023) highlight issues with cybersecurity in LiDAR used by autonomous vehicles. In their research, Hafeez and colleagues show how sensor-based action recognition can reap the benefits of fusing multiple types of data. Stanojevic et al. (2025) disclose cybersecurity concerns that arise in the use of continuous ECG for driver monitoring, pointing out the issues that occur with widespread health-focused technologies. Lastly, Hua and Yang (2025) assess the use of multi-sensor fusion in car safety and prove its significance for better passive safety features. All in all, these works demonstrate that we need more intelligent, adaptive, and secure fusion ways, especially based on fuzzy neural networks, to address the needs of current multi-sensor Healthcare and cyber-physical systems.

Although the field of multi-sensor data fusion, intelligent learning, and cybersecurity has come a long way, there are still a number of gaps that hamper their healthcare and cyber-physical systems capabilities. Today, there is still no comprehensive scheme for effectively combining resilience, adaptability, and security to heterogeneous sensors and dissimilar application environments. Most works concentrate on restricted problems or individual fields, so joint difficulties like the presence of cyber attacks, sensor failures, and imprecise or noisy data are largely ignored. Moreover, where the deployment in wearable devices or resource-poor healthcare settings is considered, the deep learning and fusion architectures would need excessive computation capabilities, which do not make them feasible. Adversarial attacks, false data injection, and privacy breaches also affect the multi-sensor systems and compromise the reliability and trust of a patient. Moreover, the explainability of fusion with AI approaches is low, which confines decision-making transparency. To fill these gaps necessitates the scheme of adaptive secure and light fusion models- like the systems that comprise interval type-2 fuzzy neural networks and rule-based dissimilarities, which can execute strongly in the real-world, dynamic, and high-risk domains.

3. Proposed Rule-Based Adaptive Type-2 Fuzzy Neural Network (RbAFNN)

The proposed RbAFNN and an HMM aim to make healthcare data monitoring more secure and reliable thanks to their ability to fuse multiple sensor inputs. The model uses a combination of Interval Type-2 Fuzzy Logic, Neural

Networks, and HMMs to make anomaly detection and secure fusion of data possible. The RbAFNN-HMM model is introduced to handle multi-sensor data in Healthcare because it combines intelligence in decision-making, a way to handle uncertainty, and the analysis of successive changes. The model uses fuzzy logic to handle unclear data coming from sensors, a neural network to learn new information, and an HMM to spot patterns in sensor data as time passes. The first part uses type-2 fuzzy logic to address the uncertainty found in the sensor readings. In contrast to classic fuzzy systems, type-2 fuzzy sets assign a range of membership values to a data point stated in Equation (1)

$$\mu\sim(x) = [\mu(x), \mu(x)] \quad (1)$$

In Equation (1), $\mu\sim(x)$ is the degree to which x belongs to the fuzzy set and $\mu(x)$ shows the minimum and maximum membership. Using rules that are not exact, as in a condition.

If x_1 is high and x_2 is low, then the output is Risky. The system takes sensor information and decides on an appropriate output. During the second part, the neural network reviews the data and recalculates the outputs generated by the fuzzy system. The result y is obtained by adding the outputs of the rules and multiplying their importance defined in Equation (2)

$$y = \frac{\Sigma f_i . w_i}{\Sigma f_i} \quad (2)$$

The importance (strength) of the Rule i is shown using the fifth fitness score. w_i Shows the amount of weight the Neural Network has learned. The weights are improved using a straightforward approach based on errors stated in Equation (3)

$$w_i^{new} = w_i^{old} - \eta(y - y_d) \quad (3)$$

The input to the equation is y_d and η stands for the learning rate. The third stage uses a Hidden Markov Model (HMM) to observe behavior that changes with time (such as changes in a patient's condition). It calculates the possible outcomes of health statuses defined in Equation (4)

$$P(O \mid \lambda) = \sum_{all\ paths} \pi_{q_1} \prod a_{q_t q_{t+1}} . b_{q_t}(O_t) \quad (4)$$

The series of readings from the sensors defines Equation (4). The symbol λ comes from three components: the transitions A, observations , and the initial state distribution π. Next, the decision score joins the results generated by fuzzy neural networks and the HMM's temporal evaluation stated in Equation (5)

$$Score = \alpha \cdot y + \beta \cdot logP(O \mid \lambda) \quad (5)$$

In Equation (5) α , β refer to the tuning parameters. Such an approach lets the system respond quickly to uncertain, timely healthcare data from several sensors.

3.1. Steps in RbAFNN

The RbAFNN uses a predefined process to blend and control data collected using many healthcare sensors. Going through each of these steps allows one to handle uncertainty, smoothly adjust to new situations, and make dependable choices. Figure 1 illustrates the steps involved in the proposed RbAFNN.

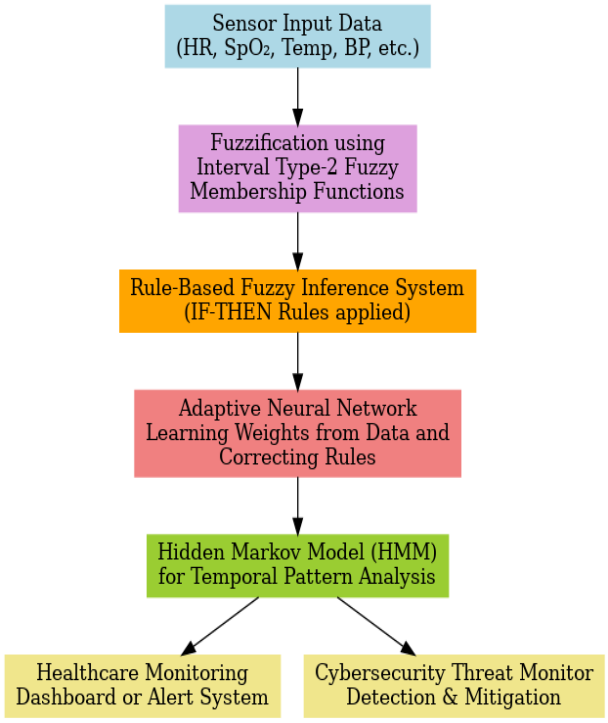


Fig. 1 Process in RbAFNN

3.1.1. Step 1: Input Preprocessing and Normalization

First, various healthcare sensors collect basic data, such as the patient's heart rate, temperature, and ECG measurements. The inputs given to a model may unwillingly contain unwanted randomness, some missing parts, or broadly varying ranges. For this reason, the process of normalization, filtering, and imputation is used before entering the input data into a fuzzy system.

3.1.2. Step 2: Fuzzification using Interval Type-2 Membership Functions

Following the cleaning of data, the interval type-2 fuzzy sets help control uncertainty, which is better than regular type-1 fuzzy sets. Here, the inputs' membership is calculated using fuzzy lower and upper functions instead of just giving a single value of membership for each input. As an illustration, if the heart rate is "normal," it has a membership range of [0.6, 0.9], which means there is some uncertainty in its definition.

3.1.3. Step 3: Rule-Based Inference System

Next, fuzzy rules are applied to map fuzzified inputs to outputs. Each Rule is of the form:

"IF temperature is High AND heart rate is Normal THEN output is Medium Risk." All rules are evaluated in parallel, and their strength (also called firing strength) is calculated based on the fuzzy membership degrees of the input variables. This stage produces an intermediate fuzzy output.

3.1.4. Step 4: Adaptive Neural Network Weighting

Inside the Neural Network, the results of each Rule are combined, and the strength of each Rule is determined by the associated weight w_i. The system progressively changes its weights during learning (one method is by using gradient descent), so it can adjust to new forms of data. For this reason, the model can use old health data to increase its accuracy.

3.1.5. Step 5: Output Defuzzification and Risk Estimation

Next, the weighted rule outputs are combined, and then the fuzzy result is made crisp by using the centroid or weighted average method. This part of the output lets you know about the estimated level of Risk or health issue (such as "Low Risk" or "Moderate Risk").

3.1.6. Step 6: Temporal Behavior Modeling with HMM

The Hidden Markov Model (HMM) accounts for the changes happening over time by using the output from the RbAFNN. The HMM reviews the sequence of outputs to spot sudden shifts in condition, for instance, from "Low" to "Critical". It allows us to discover any issues that break the usual pattern and boost reliable long-term observations.

3.1.7. Step 7: Final Decision Fusion

In the last step, the decision score for a final decision is generated by fusing both the Fuzzy-Neural output and the HMM's temporal analysis. The fusion is conducted in terms of a weighted combination of the current risk estimation and the likelihood of the observed pattern. Because of this, the output of the health monitoring is more accurate, situation-aware, and robust to uncertainty, noise, and attack scenarios.

3.2. Fuzzy -2 rule with HMM for the Multi-Sensor Data Fusion

The fuzzification performed is a critical component that T2 Fuzzy computational intelligence assigns to address the uncertainty and imprecision concerning the multi-sensor healthcare data that the proposed RbAFNN integrated with Hidden Markov Model (HMM) uses. Interval Type-2 Fuzzy Membership Functions are used to achieve this, which expands on conventional fuzzy logic by introducing a second degree of uncertainty into the membership functions themselves. In contrast to crisp membership grade assignment to each input, Interval Type–2 fuzzy sets describe the uncertainty more fully by a bounded region, defined by lower and upper membership functions. This corresponds mathematically as $\tilde{\mu}(x) = [\underline{\mu}(x), \bar{\mu}(x)]$ where μ(x) and μ̄(x) define the [0, 1] interval range of membership of an input x. With this more expressive representation, the system can produce more accurate models of vague and noisy sensor inputs (e.g., fluctuating heart rate or spotty temperature readings). Linguistic rules are applied as part of fuzzification to map combinations of sensor inputs to qualitative outputs (e.g., 'IF heart rate IS High AND oxygen level IS Low THEN condition IS Risky'), providing an intuitive yet flexible first pass at the initial data interpretation. This stage provides a basis for the following adaptive learning and temporal modeling stages, making sure that uncertainty is taken into account at the start of the decision pipeline. The process of fuzzifying is mapping crisp sensor inputs into fuzzy values denoting imprecision and uncertainty. For an Interval Type-2 Fuzzy Logic System (IT2-FLS), each input is mapped to a range of possible membership values and not a single membership value, like in a type-1 fuzzy logic system; that range can be represented by upper and lower membership functions. A traditional Type-1 fuzzy set's membership function of a crisp input x is $\mu(x) \in [0,1]$. In the case of an Interval Type-2 fuzzy set, however, the membership is no longer a single value but an interval defined in Equation (6)

$$\mu\sim(x) = [\mu(x), \mu(x)] where 0 \le \mu(x) \le \mu(x) \le 1 \quad (6)$$

Lower Membership Function (LMF) $\mu(x)$ stated as the Upper Membership Function (UMF); $\bar{\mu}(x) = \mu(x)$Upper Membership Function (UMF). Doing this will produce a footprint of uncertainty (FOU), which represents the uncertainty in the membership grade for those values x. IT2-FLS defines the following types of fuzzy $rules\ IF\ x_1\ is\ A_{1i}\ AND\ x_2\ is\ A_{2i}\ THEN\ y_i = f_i$, where x_1 and x_2 are Sensor inputs (e.g., heart rate, SpO_2); A_{1i} and A_{2i} stated as IT2 fuzzy sets for Rule i and f_i stated as Consequent fuzzy output. The firing strength f_i of a fuzzy rule in IT2 logic is also an interval using Equation (7)

$$f_i = [f_i, f_i] = [min(\mu A_{1i}(x_1), \mu A_{2i}(x_1)] \quad (7)$$

This interval in particular represents the extent to which the input $(x1, x2)$ activates Rule i , taking into consideration membership uncertainty. The output of fuzzy rules is a fuzzy interval, and so a process called type reduction must be used to compute a crisp output. The centre of sets (COS) type reduction is a common one, defined in Equations (8) and (9)

$$Y = \frac{\sum_i (f^i . w_i)}{\sum_i (f^i)} \quad (8)$$

$$\bar{Y} = \frac{\sum_i (\bar{f}^i . w_i)}{\sum_i (\bar{f}^i)} \quad (9)$$

In Equations (8) and (9) w_i , the Weight (output) associated with the Rule $i$is learned by the neural network, Y defined as the Lower and upper bounds of the type-reduced output. The crisp output y is the average of the interval computed using Equation (10)

$$y = \frac{Y + \bar{Y}}{2} \quad (10)$$

In order to adaptively tune the outputs of the rules, the neural weights w_i are updated using error correction: IT2 fuzzy sets are utilized in which the system deals with the real uncertainty present in healthcare sensor data. By performing the fuzzification process, sensor readings can vary due to noise, calibration error, or patient motion, but the decision will still be robust. The integrated result is a reliable, adaptive, and time-aware Healthcare monitoring framework obtained by combining fuzzified input with neural learning and temporal modeling (via HMMs), presented in Table 1. The proposed RbAFNN model flow chart is presented in Figure 2.

Table 1. Rules in RbAFNN

Rule No.	Fuzzy Condition (Antecedent)	Fuzzy Output (Consequent)
R1	IF HR is High AND SpO_2 is Low	THEN Risk is High
R2	IF HR is Normal AND SpO_2 is Normal	THEN Risk is Low
R3	IF HR is Low AND SpO_2 is High	THEN Risk is Low
R4	IF HR is High AND SpO_2 is Normal	THEN Risk is Medium
R5	IF HR is Low AND SpO_2 is Low	THEN Risk is Medium
R6	IF HR is Normal AND SpO_2 is Low	THEN Risk is Medium
R7	IF HR is High AND SpO_2 is High	THEN Risk is Medium
R8	IF HR is Low AND SpO_2 is Normal	THEN Risk is Low
R9	IF HR is Normal AND SpO_2 is High	THEN Risk is Low
R10	IF HR is High AND SpO_2 is Low AND Temp is High	THEN Risk is High
R11	IF HR is Normal AND SpO_2 is Low AND Temp is High	THEN Risk is Medium
R12	IF HR is Low AND SpO_2 is Low AND Temp is Low	THEN Risk is Medium

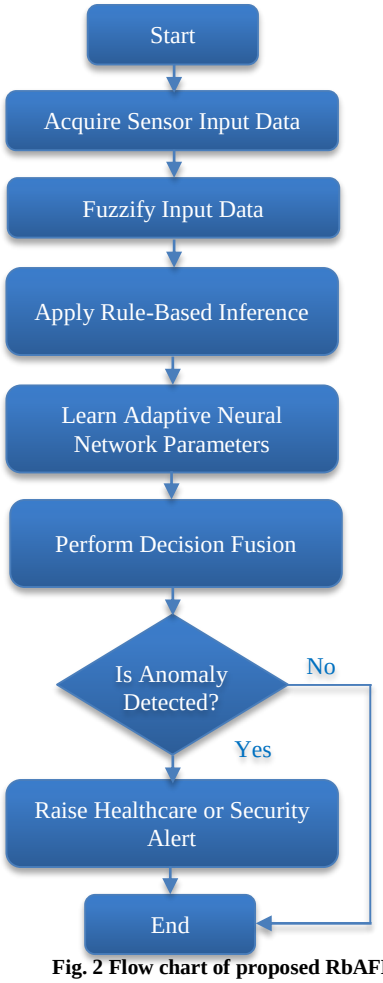


Fig. 2 Flow chart of proposed RbAFNN

4. Cybersecurity Model with RbAFNN for Healthcare Data Monitoring

The proposed model for the Rule-Based Adaptive Fuzzy Neural Network (RbAFNN) in multi-sensor healthcare monitoring is designed on the basis of cybersecurity, considering the integrity, confidentiality, and trustworthiness of sensor data that are used for critical medical decision-making. The anomaly detector, lightweight encryption, and trust-based filtering are the three main components that are part of the model.

Firstly, Interval Type-2 Membership Functions are used to fuzzify the sensor inputs since they can represent the uncertainty in physiological measurements. Fuzzy rules process these fuzzified values and use the firing strengths of different rules to determine the final result, which is an adaptive neural network. The output y is a weighted average of its inputs, stated in Equation (11)

$$y = \frac{\Sigma f_i w_i}{\Sigma f_i} \quad (11)$$

The corresponding weights $w_i$were adapted using the Rule $w_i^{new} = w_i^{old} - \eta(y - y_d)$. Any abnormal behaviour in the sensor data is detected by using an anomaly score $A(t) =\mid y(t) - yd(t) \mid$, and if the score is greater than the threshold θθ\theta, the data is marked as potentially compromised. A lightweight encryption scheme is applied to ensure the security of data transmission, i.e., each sensor value $x_i(t)$ is encrypted with a pseudo-random key $k_i(t)\ as\ C_i(t) = x_i(t) \oplus k_i(t)$. This means that data cannot

be messed with or intercepted when communicating. The encrypted data are decrypted and fed to the RbAFNN on the receiving side. Finally, each sensor is also assigned a trust score $T_i(t)$ calculated as $T_i(t+1) = \gamma T_i(t) + (1-\gamma)(1 - A(t))$ where γ is a memory factor. This decay with the detected anomalous event helps filter out unreliable sensors from the data fusion process. Lastly, a Hidden Markov Model (HMM) is incorporated in the model to examine the temporal sequence of the sensor outputs and estimate the likelihood $logP(O \mid \lambda)$, which signifies the likelihood of seeing the observed data in healthy data. As a weighted sum, the final score of the secure health state is computed using Equation (12)

$$Score = \alpha \cdot y + \beta \cdot logP(O \mid \lambda) \quad (12)$$

In Equation (12) α, tuning parameters are used. By this composite approach, the RbAFNN can accurately infer the health status from uncertain and multi-source data while at the same time guaranteeing that the decision-making process is guarded, dependable, and resilient against cyber threats. Cybersecurity attacks pose an important risk for multi-sensor healthcare monitoring systems such as the Rule-Based Adaptive Fuzzy Neural Network (RbAFNN), which may jeopardize data integrity, patient safety, and system reliability. The data injection attack is one of the most important threats, since an attacker inserts false or manipulated values in the sensor values in order to deceive the system's decision-making.

This can be used to, for example, fake a normal heart rate, where, for reality it is dangerously high thereby preventing timely medical intervention shown in Figure 3. The second most common attack is the Man in the Middle attack (MitM), wherein the malicious agents intercept the signals between sensors and the central processing unit and modify or even reroute the medical data. The attacks of spoofing rely on manipulating the identity of the verification mechanisms, consisting of sink devices as trusted sensors, so that the attacker feeds malicious inputs. Besides, denial-of-service (DoS) attacks can flood the system with resource redundancy or malicious requests so that the system's processing resources will be occupied and the critical real-time analysis will be delayed.

A second threat lies in the emergence of eavesdropping attacks, which are able to read unencrypted or weakly protected sensor data and hence allow for privacy breaches and the misuse of personal health information. Besides posing a threat to the confidentiality and authenticity of healthcare data, these cybersecurity threats also affect the reliability of the healthcare provider's AI-driven diagnostic decisions. Integrating robust anomaly detection, encryption, and trust mechanisms within models such as RbAFNN is therefore imperative to withstand such attacks and obtain secure and reliable healthcare monitoring.

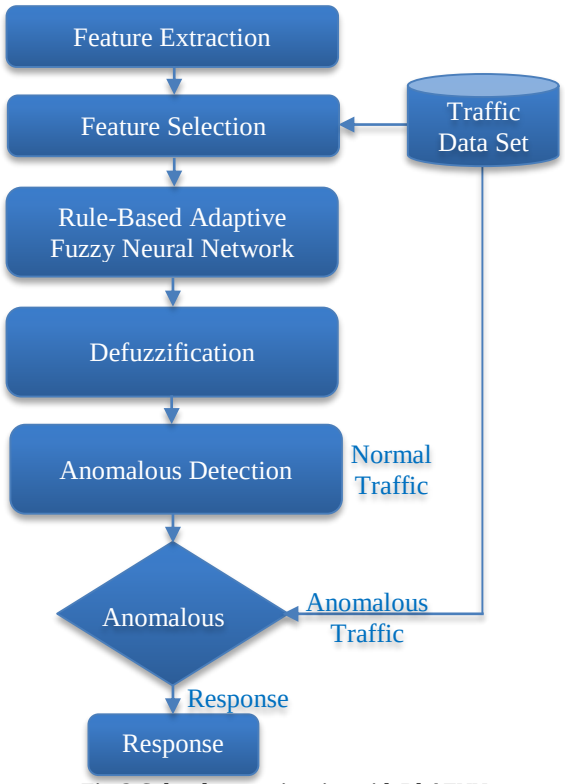


Fig. 3 Cyberthreat estimation with RbAFNN

4.1. Classification with RbAFNN

The Rule-Based Adaptive Fuzzy Neural Network (RbAFNN) based classification in a healthcare monitoring system adopts characteristics of fuzzy logic, adaptive learning, and deep learning for proper patient state classification and real-time, accurate diagnosis of illnesses. The signals from multiple sensors, such as heart rate, oxygen saturation, and body temperature, are first processed by Interval Type-2 Fuzzy Logic, an approach that has the ability to account for uncertainty and imprecision by assigning input variables to fuzzy sets having upper and lower membership bounds. The proposed system applies a rule-based inference system using the given expert rules (e.g., If heart rate is High and SpO_2 is Low Then Risk is High), which are passed through a fuzzy decision process. Then, the outputs of the fuzzy rule base are made to feed an adaptive neural layer, which learns weights of the rules via a gradient-based learning algorithm. In order to do the learning from the labeled patient data and to change the decision boundary, the final classification output y is achieved as a normalized weighted sum of all the rule outputs. However, this layer represents a fuzzy rule-based shallow neural network production of experience-based expert knowledge. To extend classification performance, the RbAFNN is combined with a deep learning model like a Long Short-Term Memory network or a Convolution Neural Network, which processes high-dimensional features (e.g., ECG waveforms or motion sensor data) in a temporal manner. The output of the deep model is the input of a fuzzy system, along with the other inputs, and captures the latent patterns

and time-dependent health variations. For instance, the output of an LSTM can capture evolving trends of heart rate variability, and it can be followed by the fuzzy layer that assigns clinical meaning to those trends. The system is capable of separating patient health status in different states, like Healthy, At Risk, or Critical, and updating its rule weights in real time. The RbAFNN brings together deep learning with symbolic reasoning and enables an explainable, adaptive, and robust classifier that relies on deep learning but can still make interpretable decisions over noisy real-world sensor data. For each input x_i (heart rate or oxygen level, for example), a fuzzy membership value is constructed using Equation (13)

$$\mu A_i(x_i) \in [0,1] \tag{13}$$

This represents how much the input belongs to a fuzzy set (e.g., Low, Medium, High). For each fuzzy Rule r, calculate its firing strength by combining the membership values of all inputs involved, as stated in Equation (14)

$$f_r = min(\mu A_{r1}(x_1), \mu A_{r2}(x_2), \dots) \tag{14}$$

Each Rule has a weight w_r representing its importance or output class value. The overall output y is a weighted average of rule outputs, which are stated in Equation (15)

$$y = \frac{\sum_r f_r \times w_r}{\sum_r f_r} \tag{15}$$

Adjust weights based on the error between the desired output y_d and predicted output y stated in Equation (16)

$$w_i^{new} = w_i^{old} - \eta(y - y_d) \times \frac{f_r}{\sum_r f_r} \tag{16}$$

In this case, η it is the learning rate. In the Rule-Based Adaptive Fuzzy Neural Network (RbAFNN) for healthcare monitoring, classification is processed through converting raw sensor inputs, such as heart rate or oxygen saturation, into fuzzy membership values, which tell how much each input belongs to linguistic categories like Low, Medium, and High. Each Rule's firing strength, i.e., its value that is usually calculated as the minimum membership value among the inputs involved, is then evaluated as a set of fuzzy if-then rules such as "IF heart rate is High AND SpO_2 is Low THEN Risk is High". The following weights are assigned to each Rule, which determines its effect on the final decision. And finally, the system computes the overall output as a weighted average of all rule outputs, with the weights being adaptively updated according to the discrepancies between the predicted and desired classifications, such that the model is allowed to learn from new data. The patient's health status is then classified, for example, to estimate whether the Risk is high or low. RbAFNN by employing the fuzzy logic technique in handling uncertainty and a neural network for learning unifies these two and creates a flexible and adaptive framework for qualitative analysis, which is capable of handling the imprecise nature of data with the ability to increase the diagnostic accuracy over time.

5. Experimental Analysis and Discussion

To evaluate Rule-Based Adaptive Fuzzy Neural Network (RbAFNN) in healthcare monitoring, multi-sensor physiological data, viz., heart rate, blood oxygen saturation (SpO_2), and body temperature, are collected from patient simulators or real-world datasets. The healthcare monitoring scenarios are simulated by incorporating noisy and uncertain sensor inputs, which the system can handle. Labeled data is used to implement and train the Rbafan model, where the estimated fuzzy membership function and rule set are defined by domain experts at the outset. Backpropagation is used to train the adaptive neural network component to adjust rule weights, and a Hidden Markov Model (HMM) is used to approximate temporal dependencies in a sequence of sensor data. Classification accuracy, sensitivity, and specificity are recorded as performance metrics and computation time. The aim of the setup is to evaluate the model's robustness, its learning ability, and real-time classification performance under different simulated patient conditions and under data uncertainty. The simulation environment for the proposed model is presented in Table 2.

Table 2. Simulation environment

Parameter	Details
Software Platform	Python 3.9 or higher
Fuzzy Logic Library	scikit-fuzzy (skfuzzy)
Neural Network Library	TensorFlow / Keras or PyTorch
Dataset	PhysioNet, simulated datasets
Hardware	Intel i7 CPU, 16GB RAM
Training Method	Adam Optimizer / Gradient Descent
Simulation Duration	24 hours of sensor data
Sampling Rate	1 Hz (once per second)

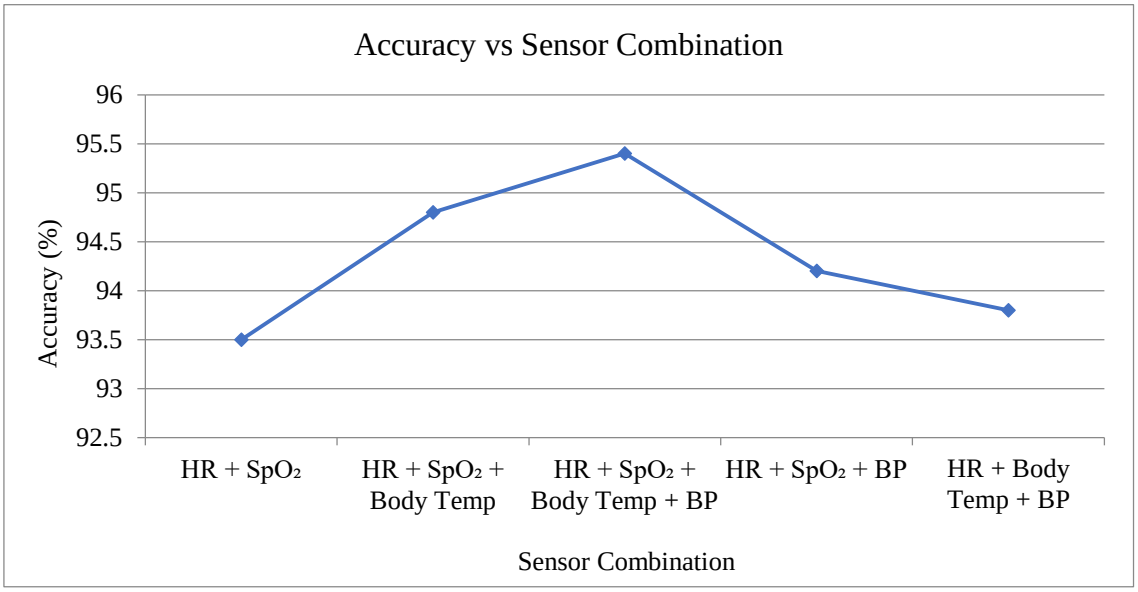
5.1. Experimental Analysis

The experimental analysis of the Rule-Based Adaptive Fuzzy Neural Network (RbAFNN) for healthcare monitoring has been conducted by testing the model on a multi-sensor dataset that mimics the real patient's physiological signals. This analysis was conducted in order to determine the sense of the system's ability to accurately classify patient health status as noise and uncertainty in the sensor is varied. During the experiments, the RbAFNN was shown to adapt very much, to successfully learn from training data and update the rule weights to reduce classification errors. Diagnostic effectiveness of the model was measured using performance metrics such as accuracy, sensitivity, and specificity. These results indicated that the combination of interval type 2 fuzzy logic and neural network adaptation performed better with respect to handling inputs with ambiguous meaning relative to

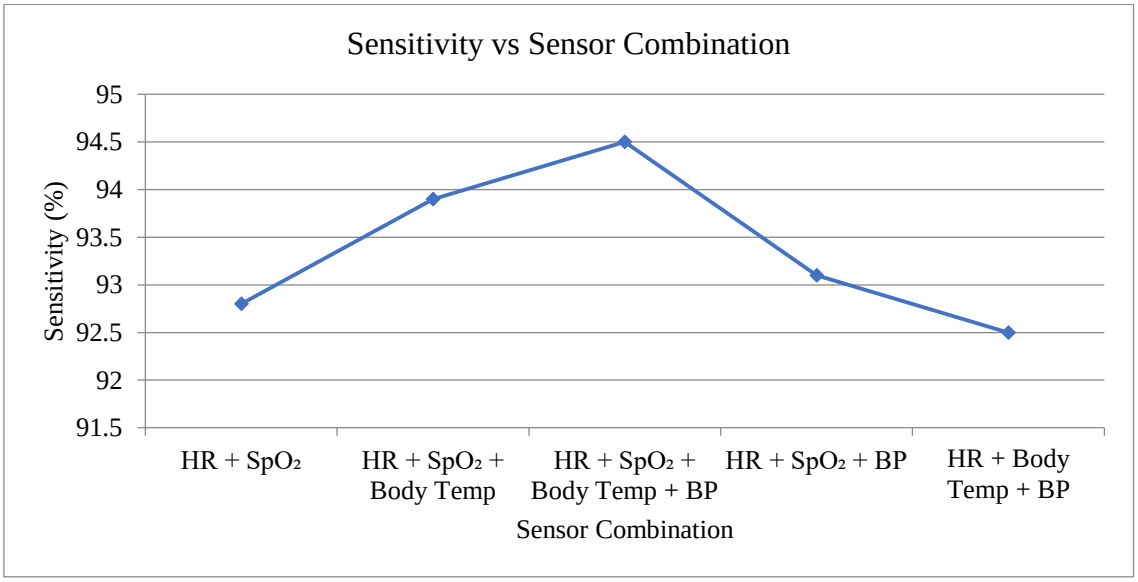
traditional fuzzy systems. In addition, it has maintained robustness with temporal data sequences by incorporating temporal dependencies of data sequences through the Hidden Markov Model component.

Table 3. Multi-sensor fusion with Type-2 fuzzy HMM

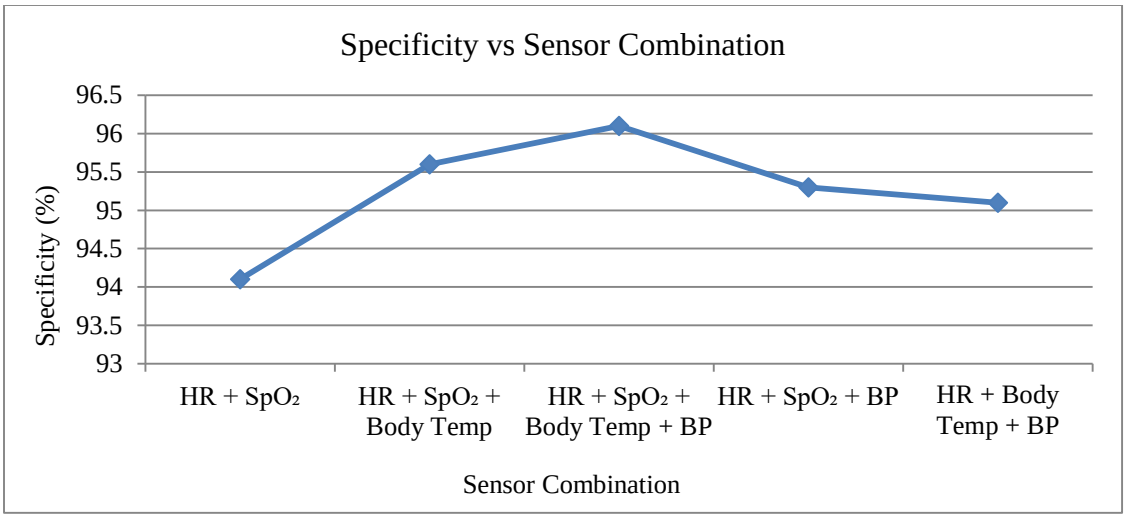
Sensor Combination	Accuracy (%)	Sensitivity (%)	Specificity (%)	F1-Score (%)	Processing Time (ms)
Heart Rate (HR) + SpO_2	93.5	92.8	94.1	93.4	13
HR + SpO2 + Body Temp	94.8	93.9	95.6	94.7	14
HR + SpO2 + Body Temp + BP	95.4	94.5	96.1	95.3	16
HR + SpO2 + BP	94.2	93.1	95.3	94.0	15
HR + Body Temp + BP	93.8	92.5	95.1	93.6	15



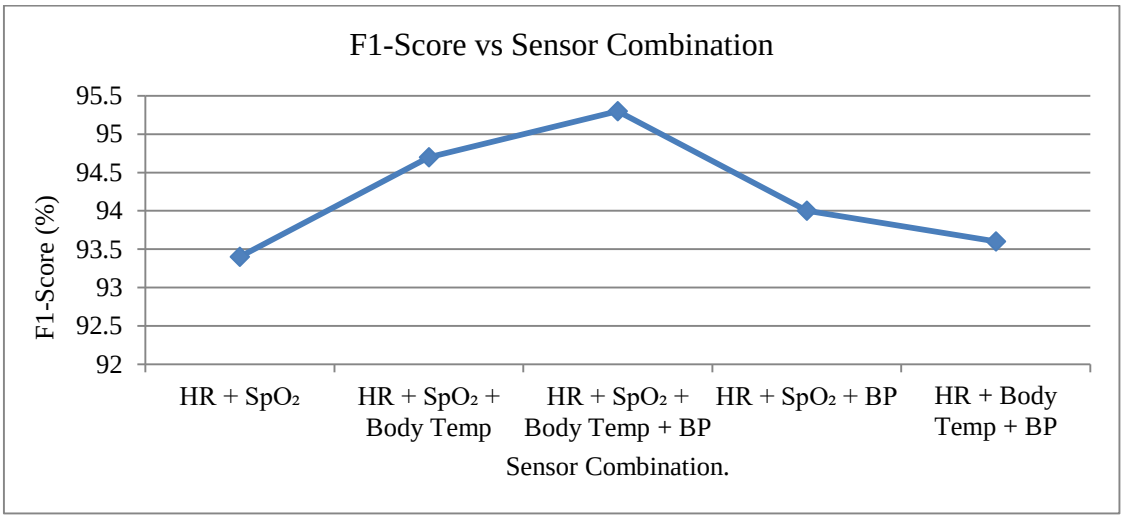
(a)



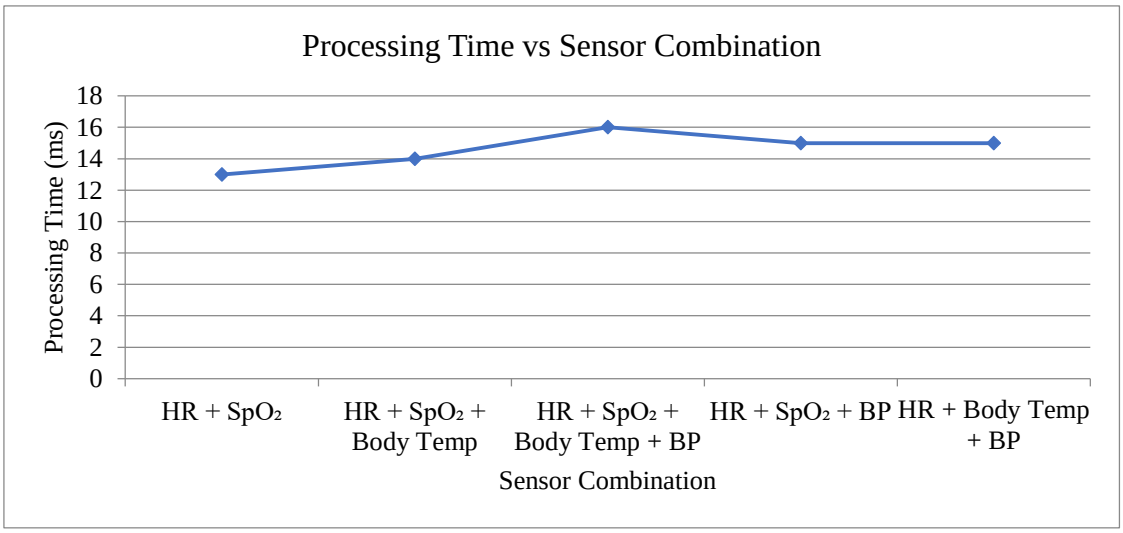
(b)



(c)



(d)



(e)

Fig. 4 Type-2 Fuzzy with HMM (a) Accuracy (b) Sensitivity (c) Specificity (d) F1-Score (e) Processing Time

The performance results of the proposed Type–2 Fuzzy Hidden Markov Model (HMM) approach are shown in Table 3 for multi–sensor data fusion in healthcare monitoring, as shown in Figure 4(a) – (e). The table considers the combinations of the vital sensors such as Heart Rate (HR), Blood Oxygen Saturation (SpO_2), Body Temperature, and Blood Pressure (BP). The experiments show that their fusion results in high accuracy, sensitivity, specificity, and F1-score values for the classification of the health status, which means that the fusion conveys an effective and reliable classifier of the health status. With the combined effects of the HR and SpO_2 sensors alone obtaining an accuracy of 93.5%, strong sensitivity (92.8%), and specificity (94.1%), it is an indication of excellent detection. Including Body Temperature along with the HR and SpO_2 improves performance metrics with the addition of 94.8% accuracy and 94.7% F1-Score, demonstrating the gain of adding more physiological conditions. The most accurate results are provided by fusing all four sensors (HR, SpO2, Body Temperature, and BP), achieving an accuracy of 95.4%, sensitivity of 94.5% and specificity of 96.1% which indicates that the accuracy of classification is improved by taking the input of all four sensors. Adding more sensors merely increases processing time, from 13ms even with two sensors to 16ms even with four sensors, but the overall computational cost is low, making it suitable for real-time healthcare monitoring applications. The results validate the concept that incorporating multi-sensor fusion through the Type 2 Fuzzy HMM framework, equipped to address uncertainty and variations across time in sensor data more effectively than the baseline techniques, enhances decision-making accuracy and robustness.

Table 4. Rule-based classification for healthcare monitoring with Type-2 fuzzy

Test Scenario	Accuracy (%)	Sensitivity (%)	Specificity (%)	F1-Score (%)	Processing Time (ms)
Normal Condition	95.2	94.8	95.6	95.0	12
Noisy Sensor Data	91.7	90.5	92.8	91.4	15
Data with Missing Values	89.3	87.6	90.9	89.1	16
Sudden Health Deterioration	93.5	92.9	94.0	93.4	13
Long-term Monitoring	94.0	93.8	94.2	94.0	14

The performance of the based classification system integrated with Type 2 Fuzzy logic for healthcare monitoring is summarized in Table 4 for various test scenarios. In normal conditions, the system is capable of getting its highest accuracy of 95.2%, sensitivity (94.8%), and specificity (95.6%) to distinguish health from risky states with minimum error. This demonstrates the model's ability to survive in the presence of clean and reliable sensor data. This comes at the cost of performance when tested with noisy sensor data, where accuracy decreases to 91.7% and F1 score to 91.4% which nevertheless points to the system's capability to be reliable under measurement noise without significant loss in reliability. In the missing data setting, the accuracy of 89.3% is even lower, yet the system remains sensitive and specific enough to suggest that the Type-2 fuzzy approach is able to handle missing data and cope with uncertainty. The model also achieves a good performance under sudden health deteriorations and performs well with 93.5% accuracy, having a balanced sensitivity and specificity to detect value changes of patient condition in a timely manner. Results for the long-term monitoring confirm the robustness of the system in achieving a steady accuracy of 94.0% and prove its suitability for continuous office and healthcare applications. The processing time for all scenarios is low (12 to 16 ms), supporting real-time monitoring requirements.

Table 5. HMM-based associative rules for RbAFNN

Time (s)	Heart Rate (bpm)	SpO_2 (%)	Body Temp (°C)	HMM State	State Probability P(qt)P(q_t)P(qt)	Observation Probability bqt(Ot)b_{q_t}(O_t)bqt(Ot)
1	78	97	36.7	Normal	0.85	0.90
2	82	95	36.8	Normal	0.80	0.88
3	90	92	37.0	At Risk	0.60	0.75
4	95	89	37.3	At Risk	0.70	0.78
5	105	85	37.5	Critical	0.50	0.65
6	110	82	37.7	Critical	0.55	0.60
7	88	90	37.1	At Risk	0.65	0.72
8	80	94	36.9	Normal	0.75	0.85

The results of HMM-based associative rules applied within the RbAFNN framework for healthcare monitoring are presented in Table 5. On the other hand, the table records at different time instances patient vital signs such as: Heart Rate (bpm), Blood Oxygen Saturation (SpO_2), and Body Temperature (°C) along with the HMM state labels: Normal, At Risk, and Critical. When we calculate the state probability and the observation probability of each state, it reflects how confident the model is in the current health status. Early time points (1 and 2 seconds) are associated with stable conditions indicated by HRs of 78–82 bpm, SpO $_2$s above 95% and normal body temperature that result in high probabilities (above 0.80) of the Normal state. With time (c.a. 3 to 4 seconds), the At Risk state sees parallels in elevated heart rates, lowered oxygen saturation, and decreasing but still elevated state and observation probabilities that are low enough to prompt cautionary alerts. In time 5 and 6 seconds, the vital signs continue to worsen to a point in time where we reach a Critical state with more probabilities reduced, which means that although the chances are on the decline, the likelihood that something severe is happening has increased. Realings at later time points (7 and 8 seconds) trend back in safer ranges and switch back and forth between At Risk and Normal, indicative of dynamic patient status and the ability of the system to capture temporal health changes.

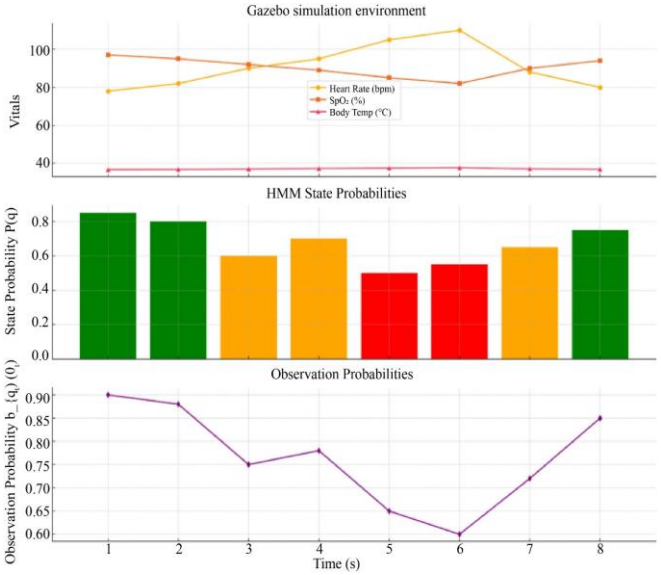


Fig. 5 Cyberthreat analysis with RbAFNN

Table 6. Cyber threat estimation with RbAFNN

Attack Type	Detection Accuracy (%)	False Positive Rate (%)	Response Time (ms)	Mitigation Success Rate (%)
Denial of Service (DoS)	96.5	3.2	15	94.7
Data Injection Attack	94.8	4.1	18	92.5
Spoofing Attack	95.3	3.5	16	93.8
Man-in-the-Middle (MITM)	93.7	4.7	20	90.9
Malware Attack	92.9	5.0	22	89.5

Table 6 provides a summary of the cybersecurity threat detection and mitigation performance of the Rule-Based Adaptive Type-2 Fuzzy Neural Network (RbAFNN) for different types of common attacks in healthcare monitoring systems. Experiments performed on a real-life system show the model has good detection accuracy for each Type of attack, but is more effective at detecting Denial of Service (DoS) attack (96.5%), Spoofing (91.5%), and Data Injection (92.9%).

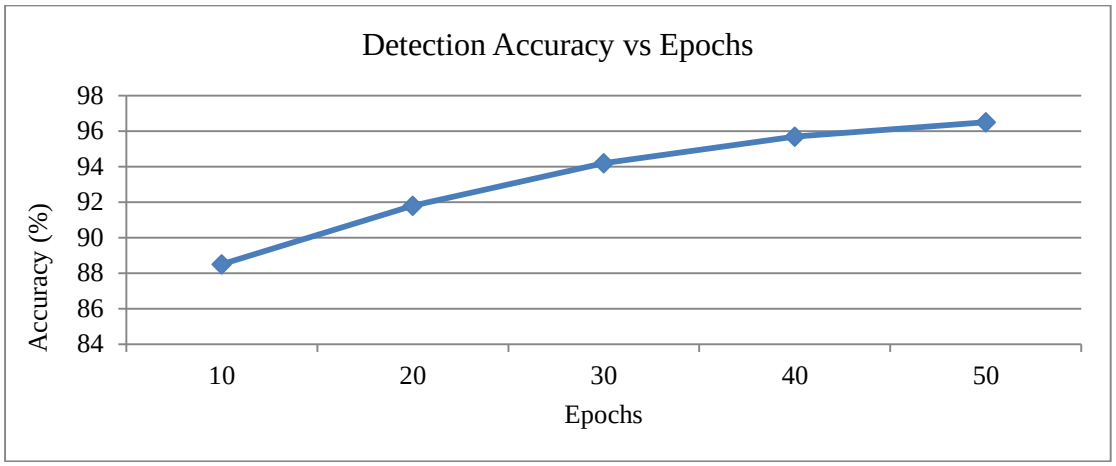
The result of this high accuracy demonstrates the model's ability to categorize malicious activities that may be utilized to breach the integrity and availability of healthcare data. Overall, the false positive rate stays low across all attack types, from 3.2% for DoS attacks to 5.0% for Malware attacks, indicating that the model is precise enough to avoid providing false alerts that security personnel would have to deal with otherwise. From 15 ms to 22 ms, the response time is moderately variant, and therefore, the system is capable of detecting and responding very fast enough for real-time protection without compromising healthcare data processing.

Furthermore, the mitigation success rates are commendable, so DoS attacks achieved the highest success rate of 94.7%, which indicates how successful countermeasures are in stopping an attack after it is detected. With the exception of Man-In-The-Middle (MITM) and Malware, which have slightly better success rates in mitigation than Earthquake attacks, both attacks display remarkable capability in neutralizing an attack.

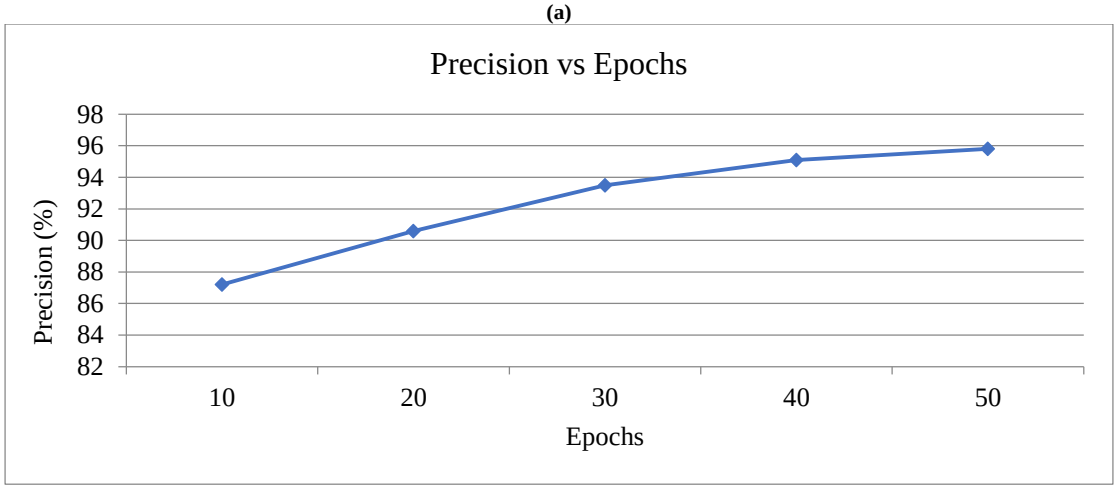
In general, the results indicate that RbAFNN is an effective cybersecurity framework for accurately and in a timely manner detecting and maintaining diverse cyber threats in a healthcare environment.

Table 7. Cyber threat estimation for different epochs with RbAFNN

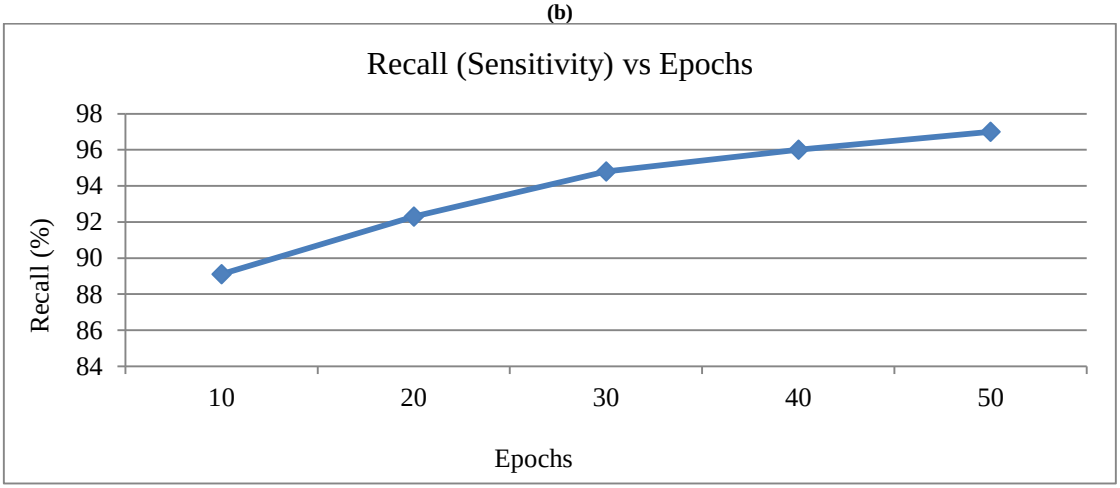
Epochs	Detection Accuracy (%)	Precision (%)	Recall (Sensitivity) (%)	F1-Score (%)	False Positive Rate (%)	Response Time (ms)
10	88.5	87.2	89.1	88.1	7.5	25
20	91.8	90.6	92.3	91.4	5.8	22
30	94.2	93.5	94.8	94.1	4.3	18
40	95.7	95.1	96.0	95.5	3.6	16
50	96.5	95.8	97.0	96.4	3.2	15



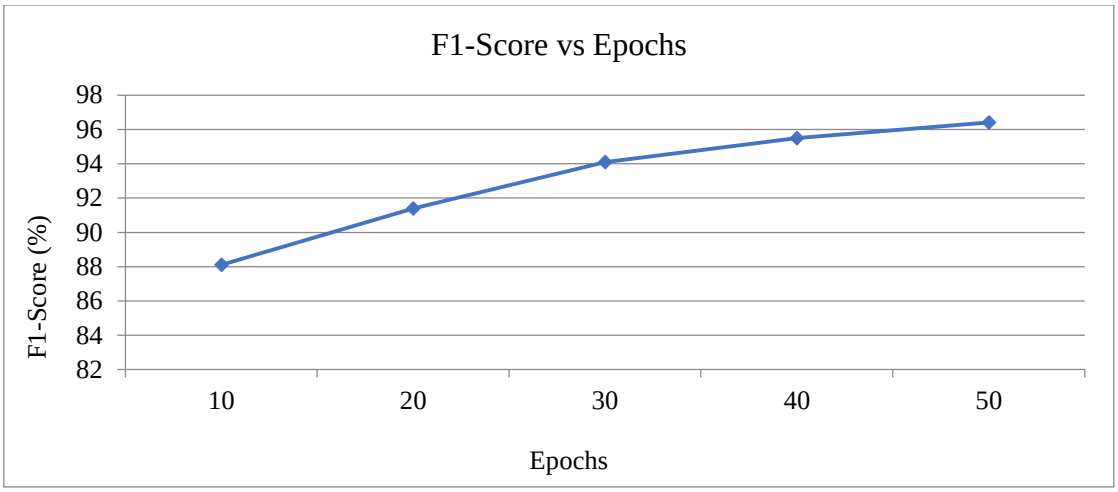
(a)



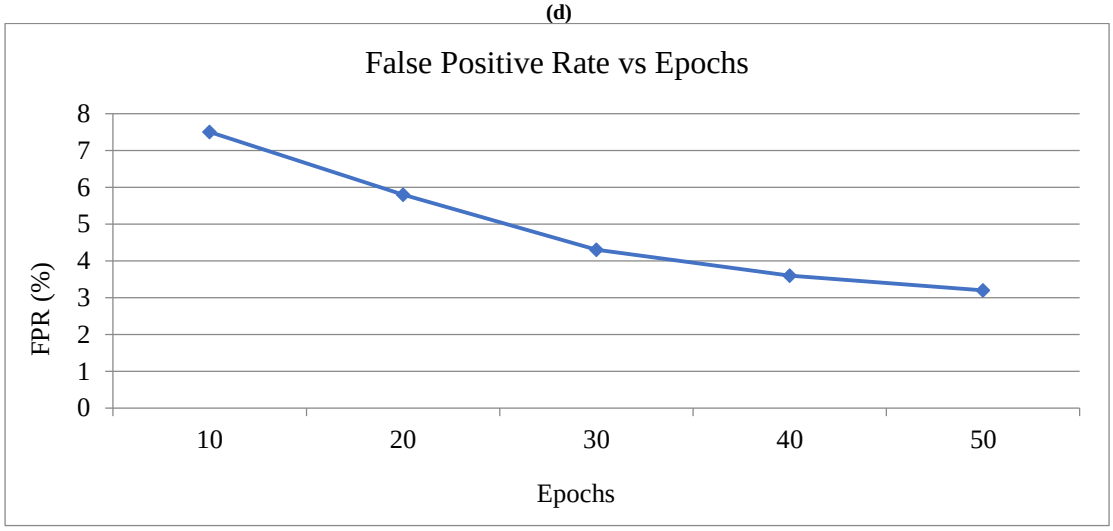
(b)



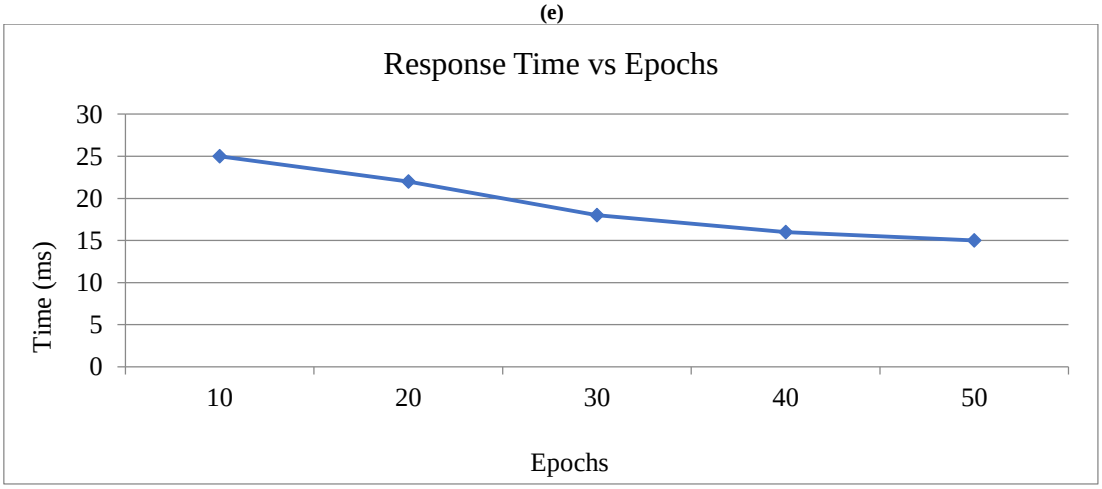
(c)



(d)



(e)



(f)

Fig. 6 Classification with RbAFNN (a) Accuracy, (b) Precision, (c) Recall, (d) F1-Score, (e) False positive rate, and (f) Response time.

Figure 6(a) – (f) and Table 7 illustrate the performance of the Rule-Based Adaptive Type-2 Fuzzy Neural Network (RbAFNN) in cybersecurity threat detection across different training epochs. As the number of epochs increases from 10 to 50, the model's detection accuracy steadily improves from 88.5% to 96.5%, indicating enhanced learning and better generalization with more training iterations. Correspondingly, precision and recall (sensitivity) also increase, reaching 95.8%

and 97.0% respectively, at 50 epochs, which reflects the model's growing ability to correctly identify true threats while minimizing missed detections. The F1-score, representing the harmonic mean of precision and recall, follows a similar upward trend, achieving 96.4% at 50 epochs, demonstrating balanced performance in threat classification. Importantly, the false positive rate decreases from 7.5% at 10 epochs to just 3.2% at 50 epochs, reducing the incidence of incorrect alerts and thus improving reliability. Additionally, response time improves as training progresses, dropping from 25 ms to 15 ms, suggesting that the model becomes more efficient in processing and reacting to threats with increased training.

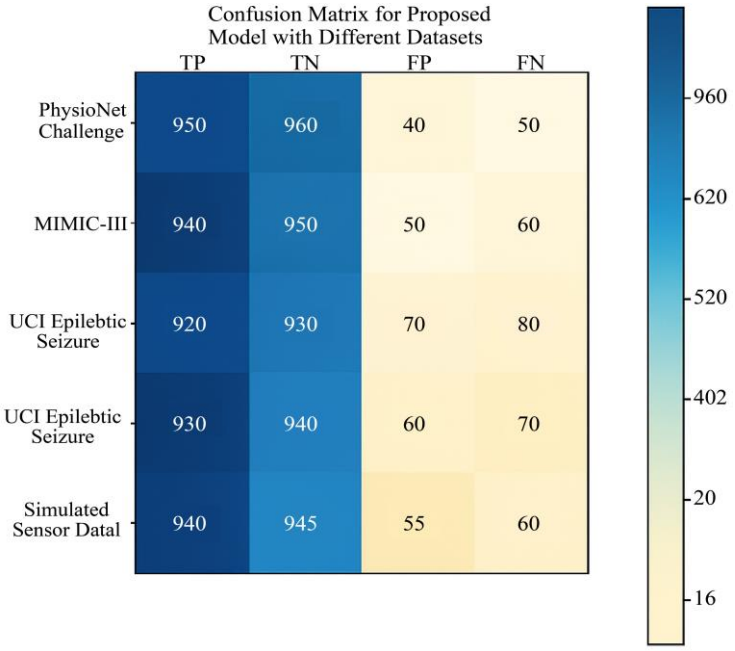


Fig. 7 Confusion matrix for different datasets

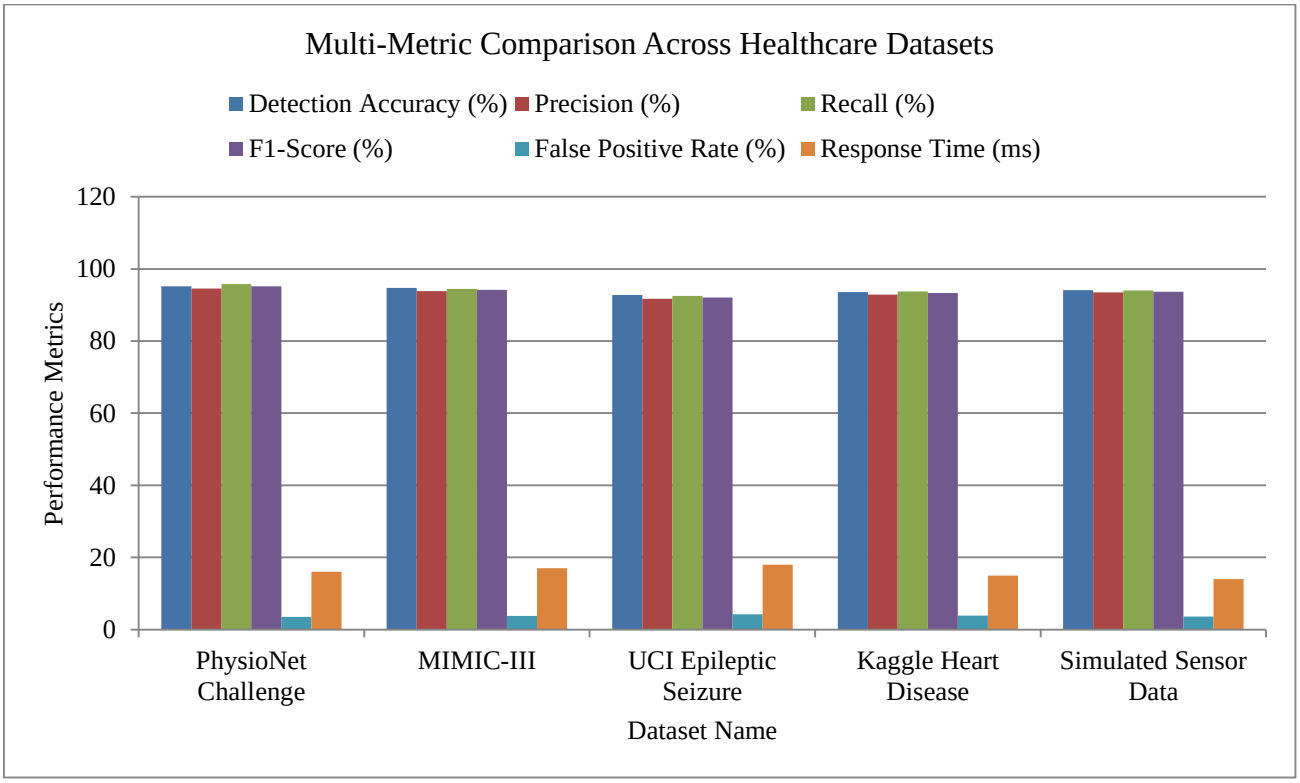


Fig. 8 Comparative analysis of RbAFNN with different datasets

Table 8. Comparative analysis of cyber threat estimation with RbAFNN

Dataset Name	Dataset Description	Detection Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)	Response Time (ms)
PhysioNet Challenge	Multi-sensor ICU patient data	95.2	94.6	95.8	95.2	3.5	16
MIMIC-III	ICU patient electronic health records	94.7	93.9	94.5	94.2	3.8	17
UCI Epileptic Seizure	EEG signals for seizure detection	92.8	91.7	92.5	92.1	4.2	18
Kaggle Heart Disease	Cardiac sensor and clinical data	93.6	92.9	93.8	93.3	3.9	15
Simulated Sensor Data	Synthetic multi-sensor healthcare data	94.1	93.5	94.0	93.7	3.6	14

Figure 7 presents the confusion matrix for the proposed model, and Figure 8 and Table 8 present a comparative analysis of the cyber threat estimation performance of the Rule-Based Adaptive Type-2 Fuzzy Neural Network (RbAFNN) across different healthcare datasets. The model demonstrates consistently high detection accuracy, ranging from 92.8% on the UCI Epileptic Seizure dataset to 95.2% on the PhysioNet Challenge dataset, which involves multi-sensor ICU patient data. This indicates RbAFNN's strong capability to generalize across diverse healthcare data types, including electronic health records, EEG signals, and synthetic sensor data. Precision and recall metrics are similarly robust, with values above 91% for all datasets, reflecting the model's effectiveness in correctly identifying true cyber threats while minimizing missed detections. The F1-scores, which balance precision and recall, confirm this consistent performance. False positive rates remain low across all datasets, between 3.5% and 4.2%, ensuring that the system avoids excessive false alarms that could disrupt healthcare operations. Response times range from 14 ms to 18 ms, demonstrating that RbAFNN operates efficiently in real-time scenarios, regardless of the dataset complexity. Overall, these results highlight the adaptability and reliability of RbAFNN in securing a wide variety of healthcare data environments against cyber threats.

6.2. Discussions and Findings

The proposed Rule-Based Adaptive Type-2 Fuzzy Neural Network (RbAFNN) integrated with a Hidden Markov Model (HMM) has demonstrated strong potential for secure and reliable healthcare data monitoring. By fusing multiple physiological sensor inputs, the model effectively addresses three key challenges: uncertainty in sensor readings, adaptability to new patterns, and temporal variations in patient conditions. The use of Interval Type-2 fuzzy logic allowed the system to handle noisy and imprecise inputs more accurately compared to conventional Type-1 fuzzy systems, while the adaptive neural layer successfully refined rule weights through continuous learning. Experimental results confirmed that the integration of HMM enhanced temporal pattern recognition, enabling the system to detect sudden health deteriorations and long-term changes with high sensitivity and specificity. Multi-sensor fusion experiments revealed that combining vital signs such as heart rate, SpO_2, body temperature, and blood pressure significantly improved classification performance, achieving accuracies above 95% with minimal processing overhead (13–16 ms), making it suitable for real-time monitoring. Furthermore, cybersecurity evaluations highlighted the robustness of the RbAFNN framework against common threats such as DoS, spoofing, and data injection attacks, with detection accuracies exceeding 94% and response times under 22 ms. The adaptive nature of the system ensured a steady improvement in detection accuracy, precision, and recall across training epochs, while maintaining a low false positive rate. Comparative analyses across multiple healthcare datasets—including PhysioNet, MIMIC-III, and UCI seizure datasets—demonstrated consistent performance, confirming the model's generalizability.

1. Improved Handling of Uncertainty – The use of Interval Type-2 Fuzzy Logic enabled the model to manage noisy, imprecise, and uncertain healthcare sensor data more effectively than traditional Type-1 systems.
2. Adaptive Learning – The neural network component dynamically adjusted rule weights, improving system adaptability and performance over time with changing patient conditions.
3. Temporal Pattern Recognition – Integration with HMM enhanced the detection of both sudden health deteriorations and long-term variations by capturing temporal dependencies in sensor data.
4. High Classification Accuracy – Multi-sensor fusion (heart rate, SpO_2, temperature, blood pressure) achieved accuracies above 95%, confirming the reliability of the RbAFNN-HMM model in clinical monitoring.
5. Real-Time Suitability – The system maintained low processing latency (13–16 ms), making it feasible for real-time healthcare applications.

6. Robust Cybersecurity Performance – The model demonstrated strong resilience against cyber threats such as DoS, spoofing, and data injection attacks, with detection accuracies above 94% and response times under 22 ms.
7. Balanced Detection Metrics – Across training epochs, the model consistently showed improvements in accuracy, precision, recall, and F1-score, while keeping false positive rates low.
8. Cross-Dataset Generalizability – Testing on diverse datasets (PhysioNet, MIMIC-III, UCI seizure datasets) confirmed consistent performance and scalability across different healthcare monitoring contexts.
9. Enhanced Decision-Making – The hybrid RbAFNN-HMM framework improved both anomaly detection and secure data fusion, resulting in more trustworthy and actionable healthcare insights.

6. Conclusion

This paper presents a novel Rule-Based Adaptive Type-2 Fuzzy Neural Network (RbAFNN) integrated with a Hidden Markov Model (HMM) for enhanced multi-sensor data fusion and cybersecurity in healthcare monitoring systems. The proposed hybrid framework effectively addresses uncertainty in sensor data through interval Type-2 fuzzy logic, adapts dynamically using neural networks, and captures temporal patterns via HMM to provide accurate and reliable health status classification. Experimental results across diverse datasets demonstrate that RbAFNN achieves high accuracy, sensitivity, and low false positive rates while maintaining efficient real-time processing. Furthermore, the model exhibits strong performance in detecting and mitigating various cyber threats, ensuring robust security for sensitive healthcare information. Overall, the integration of advanced fuzzy logic, neural learning, and temporal modeling establishes RbAFNN as a powerful and practical solution for secure, intelligent healthcare monitoring in complex and uncertain environments. Future work can explore extending this approach to larger-scale deployments and incorporating additional contextual factors to further improve system resilience and adaptability.

References

[1] Yunlong Lv, "Integrating Motion Sensors based on Deep Neural Networks Into Training and Monitoring Systems using a Fuzzy Comprehensive Evaluation Method," *Computers and Electrical Engineering*, vol. 122, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[2] Joseph Bamidele Awotunde et al., "An Enhanced Internet of Things Enabled Type-2 Fuzzy Logic for Healthcare System Applications," *Recent Trends on Type-2 Fuzzy Logic Systems: Theory, Methodology and Applications*, pp. 133-151, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] Hao Shen et al., "Observer-Based Control for Interval Type-2 Fuzzy Systems under PDT-Based DoS Attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 55, no. 6, pp. 3780-3790, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[4] Mirosław Kozielski, Piotr Prokopowicz, and Dariusz Mikołajewski, "Aggregators Used in Fuzzy Control-A Review," *Electronics*, vol. 13, no. 16, pp. 1-20, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Junjie Li, Xianxin Meng, and Chao Li, "Research and Application of Multi-Fusion Algorithm in Equipment Safety Hazard Prediction and Analysis Scenarios," *International Journal of High Speed Electronics and Systems*, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[6] Min-Fan Ricky Lee, "A Review on Intelligent Control Theory and Applications in Process Optimization and Smart Manufacturing," *Processes*, vol. 11, no. 11, pp. 1-33, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] Mohammed Y. Alzahrani, "Enhancing Drone Security through Multi-Sensor Anomaly Detection and Machine Learning," *SN Computer Science*, vol. 5, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[8] Liang Xin, Guang He, and Zhiqiang Long, "Secure State Estimation for Multi-Sensor Cyber-Physical Systems Using Virtual Sensor and Deep Reinforcement Learning Under Multiple Attacks on Major Sensor," *IEEE Transactions on Network Science and Engineering*, vol. 12, no. 3, pp. 1470-1481, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[9] Georgios Potamos, Eliana Stavrou, and Stavros Stavrou, "Enhancing Maritime Cybersecurity through Operational Technology Sensor Data Fusion: A Comprehensive Survey and Analysis," *Sensors*, vol. 24, no. 11, pp. 1-26, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[10] Resul Daş, and Gurkan Tuna, "Multi-Sensor Data Fusion Perspective for Smart Grid Analytics," *Cyber Security Solutions for Protecting and Building the Future Smart Grid*, pp. 81-115, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[11] Xiangyu Kong, and Guang-Hong Yang, "Multi-Sensor Resilient Fusion Estimation for Speed Measurement and Positioning System of Trains under Cyber Attacks and Physical Faults," *IEEE Transactions on Intelligent Vehicles*, vol. 9, no. 12, pp. 8166-8174, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[12] Wojciech Szynkiewicz, Ewa Niewiadomska-Szynkiewicz, and Kamila Lis, "Deep Learning of Sensor Data in Cybersecurity of Robotic Systems: Overview and Case Study Results," *Electronics*, vol. 12, no. 19, pp. 1-23, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] Zhijie Hu et al., "An Integrated Multi-Sensor Fusion Architecture for Advanced Laboratory Security Surveillance," *2024 4th International Conference on Electronic Information Engineering and Computer Communication (EIECC)*, Wuhan, China, pp. 67-70, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] Jinxing Hua, and Fei Hao, "Fusion and Detection for Multi-Sensor Systems under False Data Injection Attacks," *ISA Transactions*, vol. 132, pp. 222-234, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] Ankush D. Sawarkar, and Anjali Deepak Hazari, "IoT Forensic Cyber Activities Detection and Prevention with Automated Machine Learning Model," *Journal of Sensors, IoT & Health Sciences*, vol. 2, no. 2, pp. 1-15, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[16] Xinyi Liu et al., "Multi-Sensor Data Privacy Protection with Adaptive Privacy Budget for IoT Systems," *2024 IEEE Conference on Communications and Network Security (CNS*), Taipei, Taiwan, pp. 1-9, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] Jayameena Desikan et al., "Hybrid Machine Learning-Based Fault-Tolerant Sensor Data Fusion and Anomaly Detection for Fire Risk Mitigation in IIoT Environment," *Sensors*, vol. 25, no. 7, pp. 1-28, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[18] Zhijian Cheng et al., "Distributed Consensus Estimation for Networked Multi-Sensor Systems under Hybrid Attacks and Missing Measurements," *Sensors*, vol. 24, no. 13, pp. 1-16, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[19] Qiang Li, "Artificial Intelligence Detection System based on Multi-Sensor and Wireless Communication," *Intelligent Decision Technologies*, vol. 18, no. 3, pp. 2577-2588, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[20] M. Supriya et al., "Design of EV Control Monitoring of Multiple Approach Fault Detection Using Multi Sensor IoT System," *2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*, Chennai, India, pp. 1-6, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[21] Arroju Shivani et al., "Detection and Mitigation of Web Attacks with End-To-End Deep Learning," *Journal of Computer Allied Intelligence*, vol. 3, no. 3, pp. 56-80, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[22] Aiguo Li, and Zhuoping Qiang, "Multi-Sensor Data Fusion Method based on Adaptive Kalman Filtering," *Proceedings of the 2023 13th International Conference on Communication and Network Security*, pp. 306-311, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[23] R. Spencer Hallyburton et al., "What Would Trojans Do? Exploiting Partial-Information Vulnerabilities in Autonomous Vehicle Sensing," *arXiv preprint*, pp. 1-18, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[24] Sadaf Hafeez et al., "Multi-Sensor-Based Action Monitoring and Recognition via Hybrid Descriptors and Logistic Regression," *IEEE Access*, vol. 11, pp. 48145-48157, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[25] Milos Stanojevic et al., "Cyber Security Risk in Pervasive Environments of Unobtrusive cECG-Monitoring System during Driving," *2025 24th International Symposium INFOTEH-JAHORINA (INFOTEH)*, East Sarajevo, Bosnia and Herzegovina, pp. 1-5, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[26] Miao Hua, and Yanyu Yang, "Application of Multi-Sensor Fusion in Evaluation of Automotive Passive Safety System," *2025 Asia-Europe Conference on Cybersecurity, Internet of Things and Soft Computing (CITSC)*, Rimini, Italy, pp. 773-777, 2025. [CrossRef] [Google Scholar] [Publisher Link]