

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

CHAPTER 1

INTRODUCTION

1.1 Overview

The integration of Internet of Things (IoT) technology into the medical industry has revolutionized healthcare delivery by enabling real-time monitoring, predictive diagnostics, and remote patient care. According to MarketsandMarkets, the global IoT in healthcare market is projected to reach USD 254.2 billion by 2026, growing at a CAGR of 19.8% from 2021. In the United States alone, over 60% of hospitals have incorporated IoT-based medical devices into their operations to streamline patient management and automate diagnostics.

Despite the promising benefits, the rising number of connected devices has introduced complexities in managing device performance and ensuring their reliability. Studies have shown that up to 15% of medical IoT devices are prone to undetected malfunctions that can affect clinical workflows and patient outcomes. These devices often function in environments that demand high uptime and zero tolerance for delays or faults, making real-time monitoring and fault detection an essential part of hospital IT systems.

Medical IoT devices operate continuously and generate vast amounts of data across diverse parameters such as temperature, pressure, and patient vitals. Ensuring the accuracy, availability, and reliability of these devices has become critical. Efficient classification and analysis of their operational states—normal or anomalous—are necessary to preempt failures and minimize disruptions. Given the life-critical nature of many medical applications, there is an urgent need to move beyond reactive diagnostics to predictive and intelligent monitoring frameworks.

1.2 Research Motivation

In practical hospital environments, devices such as ventilators, infusion pumps, cardiac monitors, and wearable sensors are essential to patient care and must remain in optimal working condition. Companies like Medtronic, GE Healthcare, and Philips rely heavily on predictive maintenance strategies to monitor the health of these

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

devices. A malfunction in even one device can delay treatment or lead to serious medical errors, highlighting the criticality of reliable state classification mechanisms.

Hospitals and medical equipment manufacturers increasingly recognize the importance of data-driven analytics in their operational workflows. Data collected from sensors embedded in medical devices can help uncover latent issues that manual inspection may miss. For example, GE Healthcare employs cloud-based analytics to monitor imaging equipment performance across various hospitals, preventing downtime through early fault detection. Similarly, Siemens Healthineers leverages device telemetry data to maintain consistent operational quality and reduce maintenance costs.

The demand for intelligent monitoring systems extends beyond hospitals to remote patient monitoring services and elderly care homes. Real-time fault identification in wearable health trackers, glucose monitors, and smart beds enables caregivers to respond proactively. As device networks grow more complex, analyzing device data for state classification becomes not only a technical challenge but a business necessity. Data analytics ensures operational efficiency, patient safety, and long-term cost savings, which is why institutions are investing in scalable, automated diagnostic solutions.

1.3 Problem Definition

In the medical industry, IoT devices are often deployed in dynamic environments that require continuous operation and real-time data collection. However, many of these devices are vulnerable to faults, anomalies, and unexpected failures that are difficult to detect using traditional rule-based systems. The presence of noise, inconsistent sensor behavior, and unstructured logs further complicates timely identification of device states.

Manual inspection and conventional diagnostic tools fall short in detecting transient anomalies or subtle degradation trends that may not trigger alarms but still compromise performance. Moreover, existing systems often rely on scheduled maintenance or static thresholds, which fail to capture contextual behaviors or evolving device conditions. This leads to inefficiencies, higher operational costs, and risks to patient safety.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

There is a pressing need for a dynamic, data-driven method to classify the operational state of IoT devices accurately. Such a method should differentiate between normal and anomalous behavior in real-time, work across a wide range of medical device types, and adapt to data variability without relying on manual thresholds or predefined fault rules.

1.4 Significance

Medical IoT device reliability is foundational to quality healthcare delivery. An intelligent classification system for device states can minimize downtime, reduce maintenance costs, and ensure timely medical interventions. By understanding device behavior patterns, healthcare institutions can prevent minor faults from escalating into critical failures. Moreover, automatic classification contributes to a more efficient allocation of technical support, enabling staff to focus on high-priority tasks and improving the overall patient care experience.

1.5 Research Objective

The primary research objective is to design a robust, data-driven classification model capable of distinguishing between normal and anomalous states of medical IoT devices using intelligent learning techniques. The goal is to enhance device monitoring systems with a hybrid approach that captures hidden patterns and ensures precise state prediction, even in complex and non-linear data environments.

1.6 Advantages

- Enables real-time monitoring and detection of faults in medical IoT devices, ensuring uninterrupted operation in critical environments.
- Reduces manual effort and human error by automating device state classification and anomaly detection processes.
- Enhances patient safety by ensuring medical devices function correctly and provide accurate readings.
- Minimizes equipment downtime through early detection of performance degradation and impending failures.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

- Supports scalable deployment across multiple device types and healthcare environments without custom configuration.
- Provides actionable insights to biomedical engineers and hospital administrators for efficient device management.
- Adapts to changes in device behavior over time by learning from historical data patterns.
- Lowers long-term operational costs by reducing emergency maintenance and extending device lifespan.
- Improves compliance with healthcare regulations by maintaining reliable device performance and audit-ready logs.
- Facilitates integration with existing hospital IT infrastructure, supporting broader digital transformation initiatives.

1.7 Applications

- Continuous performance monitoring of infusion pumps, ventilators, and patient monitoring devices in ICU settings.
- Predictive maintenance in hospital asset management systems to reduce unexpected equipment failures.
- Remote health monitoring systems for chronic patients, identifying device or sensor anomalies in home care setups.
- Integration into smart hospital frameworks for seamless operation of interconnected IoT medical devices.
- Automated anomaly alerts in elderly care homes using wearable health trackers and fall detection sensors.
- Monitoring diagnostic equipment like MRI, CT, and X-ray machines to ensure imaging accuracy and uptime.
- Health analytics platforms used by companies like Philips or GE Healthcare to support condition-based maintenance.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

- Ensuring sensor accuracy in surgical robots or robotic-assisted procedures for precision interventions.
- Smart ambulance systems where medical equipment health status is continuously tracked during transit.

1.8 Performance Evaluation

The performance evaluation of the proposed Artificial Neural Network (ANN) model combined with an Extra Trees Classifier and the existing Gaussian Naive Bayes Classifier (NBC) is conducted using four key metrics: **Accuracy**, **Precision**, **Recall**, and **F1-Score**. These metrics assess the effectiveness of the models in classifying IoT device states as "Normal" or "Anomaly" in the context of medical industry applications. The evaluation is based on the implementation provided in the Tkinter-based GUI application, where the models are trained, tested, and compared on a dataset with the target variable attack. Below, each metric is defined with its formula and its significance in the context of the project.

1. Accuracy

- **Definition:** Accuracy measures the proportion of correctly classified instances (both Normal and Anomaly) out of the total instances in the test set. It provides an overall view of the model's performance across all classes.
- **Formula:**

$$Accuracy = \frac{TP+NP}{(TP+NP+FP+FN)}$$

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

2. Precision

- **Definition:** Precision measures the proportion of correctly predicted positive instances (Anomaly) out of all instances predicted as positive. It reflects the model's ability to avoid false positives.
- **Formula:**

$$Precision = \frac{TP}{(TP+FP)}$$

3. Recall

- **Definition:** Recall (also known as Sensitivity or True Positive Rate) measures the proportion of actual positive instances (Anomaly) that are correctly identified. It indicates the model's ability to detect all relevant anomalies.
- **Formula:**

$$Recall = \frac{TP}{(TP+FN)}$$

4. F1-Score

- **Definition:** The F1-Score is the harmonic mean of precision and recall, providing a balanced measure of a model's performance, especially when classes are imbalanced. It is particularly useful when both false positives and false negatives are costly.
- **Formula:**

$$F1 - Score = 2 \times \frac{(Precision \times Recall)}{(Precision + Recall)}$$

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

1.9 Organizational Thesis

This thesis is structured into comprehensive chapters, each elaborating on specific stages of the research and development of an Artificial Neural Network (ANN) model for classifying IoT device states in the medical industry. The aim is to provide a clear and methodical understanding of the complete process, from conceptualization to implementation and evaluation.

Chapter 1: introduces the background and motivation behind the research, defines the problem, outlines the objectives, and emphasizes the significance and scope of using ANN models in classifying the states of medical IoT devices.

Chapter 2: presents a detailed literature review, covering existing traditional methods, machine learning approaches, and recent advances in the classification of IoT device states, particularly in healthcare settings.

Chapter 3: explores conventional techniques previously used for device state monitoring, highlighting their limitations and the need for intelligent systems. This chapter also explains why ANN is chosen over other models.

Chapter 4: describes the proposed system architecture, including data collection, preprocessing, and the design and development of the ANN model used for classification.

Chapter 5: includes Unified Modeling Language (UML) diagrams such as use case, class, and sequence diagrams to visually depict the structure and behavior of the system.

Chapter 6: provides a list of software and hardware tools utilized in the development process. It includes specifics on the Python libraries, frameworks, and system configurations required. And also the installation process of python.

Chapter 7: dedicated to outlining the functional requirements of the system, which are essential in defining the intended behavior and operations of the proposed ANN-

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

based classification model for IoT device states in the medical industry. These requirements serve as a blueprint, specifying what the system should do across all phases of development — from analysis and design to implementation, testing, deployment, and maintenance.

Chapter 8: presents the complete source code with appropriate comments, providing insight into the implementation logic and methodology used in the project.

Chapter 9: focuses on the experimental results and performance analysis. It includes accuracy, precision, recall, F1-score, and confusion matrix results obtained during model evaluation.

Chapter 10: serves as the final and culminating part of the thesis, providing a comprehensive conclusion to the research while also highlighting the potential future scope for enhancing and expanding the work. This chapter synthesizes the key findings, evaluates the performance of the models used, and identifies opportunities for future development in the area of IoT device state classification within the medical industry.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

CHAPTER 2

LITERATURE SURVEY

2.1 Literature Review

Akhtar et al. [1] The rapid growth of the Internet of Things (IoT) has revolutionized healthcare by enabling continuous monitoring through sensor-based networks. However, the vast amount of data generated presents challenges in efficient classification, data routing, and feature selection. Traditional machine learning and big data approaches such as Fuzzy classifiers, K-nearest neighbors (KNN), and single-layer neural networks have been explored to address classification issues in IoT healthcare, but many suffer from limitations in scalability, accuracy, and computational efficiency. Recent works have employed hybrid algorithms and optimization techniques for better feature selection and data processing. For instance, models like LFR-CM+Fuzzy and MR-FI-ELM+SLFN have shown promising improvements using fuzzy logic and ensemble learning under the MapReduce framework. However, these approaches often fail to achieve high throughput and energy efficiency simultaneously. To overcome these limitations, this paper proposes a novel Dragonfly Rider Competitive Swarm Optimization (DRCSO)-based Deep Residual Network (DRN) model. It introduces a hybrid DROA (Dragonfly + Rider Optimization Algorithm) for feature selection and an enhanced training algorithm for the deep learning model using a combination of DA, ROA, and Competitive Swarm Optimization. The model also integrates Multi-objective Fractional Gravitational Search Algorithm (FGSA) for efficient data routing in simulated IoT networks. By applying the DRCSO-DRN model in a MapReduce framework, the authors achieve a classification accuracy of 92.9%, average residual energy of 0.086J, and throughput of 86.585, outperforming previously established methods. This literature reflects the growing interest in optimization-integrated deep learning for scalable and accurate IoT healthcare systems.

Jae Dong et al. [2] integration of IoT systems into smart healthcare infrastructures, the security vulnerabilities in medical IoT devices have emerged as a critical concern. Traditional studies have largely focused on intrusion detection methods using

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

standard testbed simulations or public datasets like NSL-KDD. While these approaches have contributed to foundational understanding, they often lack applicability to real-world medical settings due to their reliance on synthetic or generic data. Machine learning techniques such as naïve Bayes, support vector machines (SVM), and logistic regression have been widely explored for intrusion detection. However, these methods often fall short in capturing the dynamic and complex patterns found in actual healthcare environments. Furthermore, most prior works utilize binary or limited classification systems, which do not effectively differentiate the severity of detected threats. To overcome these limitations, this study proposes a novel Multi-class Classification-based Intrusion Detection Model (M-IDM), built specifically for healthcare IoT networks. The model is trained using real network data collected from active medical devices like electrocardiograms and thermometers in the National Cancer Center, South Korea. The architecture employs convolutional neural networks (CNNs), which have shown superior performance over traditional algorithms in pattern recognition and classification tasks. Unlike previous research, M-IDM introduces a multi-class labeling approach—Critical, Informal, Major, and Minor—offering granular insights into potential intrusions. Experimental results demonstrate that the CNN-based model significantly outperforms conventional algorithms in terms of detection accuracy and classification precision. This study marks an important shift toward real-device, real-data-driven intrusion detection in medical IoT systems.

Vakili et al. [3] The performance evaluation of machine learning (ML) and deep learning (DL) algorithms in IoT domains has gained significant attention due to the complex and heterogeneous nature of IoT data. Various studies have explored algorithm effectiveness on balanced and unbalanced datasets, emphasizing the importance of selecting appropriate models depending on data characteristics. Random Forest (RF) has been widely reported as a robust classifier, demonstrating superior accuracy and balanced precision-recall metrics across diverse datasets, as supported by recent empirical findings. However, RF and Decision Trees (DT) are often prone to overfitting, especially in small datasets. Algorithms like K-Nearest Neighbors (KNN) and Support Vector Machines (SVM) also show competitive performance, particularly in binary classification problems, often matching or

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

surpassing RF in terms of precision and recall. In contrast, Gaussian Naive Bayes (GNB) is noted for its minimal execution time but generally yields poorer predictive accuracy. Deep learning models, including Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), and Long Short-Term Memory networks (LSTM), exhibit higher computational costs but provide advantages in handling complex feature representations, especially in large-scale datasets. Several works have highlighted CNN's ability to outperform ANN and LSTM in execution time while maintaining comparable accuracy, although deep models often struggle with small or unbalanced datasets typical in IoT environments. Recent experiments underline the importance of convergence speed in IoT applications, where models must learn efficiently from gradually accumulating data. RF consistently demonstrates fast convergence and robust performance, while deep learning methods require more data and time to achieve similar accuracy. Furthermore, the impact of feature selection, such as the removal of biasing features, is crucial in achieving reliable model performance. Metrics like ROC-AUC alongside precision, recall, and F1-score provide a comprehensive understanding of algorithm effectiveness. The literature suggests that hybrid approaches and ensemble methods can further enhance predictive capabilities in IoT device state classification, paving the way for future research focusing on optimizing both accuracy and computational efficiency.

Saif et al. [4] Intrusion Detection Systems (IDS) for IoT environments, especially in sensitive domains like healthcare, have become critical due to the increasing number of cyber-attacks targeting cloud-based data storage. Traditional IDS approaches struggle with the high dimensionality of IoT data, making feature selection an important step to reduce computational complexity. Metaheuristic algorithms such as Genetic Algorithm (GA), Particle Swarm Optimization (PSO), and Differential Evolution (DE) have been extensively applied for optimal feature selection in IDS to enhance detection accuracy while minimizing processing overhead. Supervised learning algorithms like k-Nearest Neighbors (kNN) and Decision Trees (DT) have been widely used for classification of normal and attack traffic due to their interpretability and reasonable performance on network intrusion datasets such as NSL-KDD. Hybrid models combining metaheuristic feature selection with machine learning classifiers show promising improvements in accuracy and efficiency. Among

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

these, GA coupled with DT has been reported to outperform other combinations by effectively selecting key features that distinguish attack types such as DoS, U2R, R2L, and Probe, improving classification rates significantly. Recent studies also focus on balancing accuracy with execution time and resource utilization, which are critical in IoT healthcare where real-time detection and low overhead are necessary. The NSL-KDD dataset remains a popular benchmark for evaluating IDS algorithms, offering diverse attack classes and real-world network traffic patterns. Comparative analyses indicate that hybrid metaheuristic-machine learning systems surpass standalone classifiers in handling imbalanced and complex data. Furthermore, the integration of such hybrid IDS into IoT healthcare architectures ensures the protection of Electronic Health Records (EHR) by detecting anomalous behaviors early. Advances in simulation environments using MATLAB and Python facilitate effective testing and validation of these systems. Overall, the convergence of metaheuristic optimization and machine learning classification represents a robust approach for enhancing security in IoT-based healthcare applications.

Alsalman et al. [5] Anomaly detection plays a vital role in various fields such as cybersecurity, healthcare monitoring, and network management, where identifying rare or unusual patterns is essential for maintaining system integrity. Traditional machine learning algorithms like Support Vector Machine (SVM), K-Nearest Neighbors (KNN), and Random Forest (RF) have been widely adopted for anomaly detection due to their effectiveness in classification tasks. However, these individual models often face limitations such as sensitivity to noise, overfitting, or inability to capture complex data distributions. Ensemble learning methods, which combine multiple classifiers, have shown significant promise in overcoming these drawbacks by leveraging the strengths and compensating for the weaknesses of individual models. Previous research has demonstrated that ensemble approaches, such as bagging, boosting, and stacking, improve accuracy and robustness in anomaly detection tasks compared to single models.

Multi-Layer Perceptron (MLP), a type of neural network, has been increasingly integrated with traditional algorithms in ensembles to capture non-linear patterns and enhance detection capabilities. Studies highlight that hybrid models combining decision tree-based methods (like RF), instance-based methods (like KNN), and

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

neural networks offer improved precision and recall in detecting anomalies. Recent works also emphasize the importance of evaluating ensemble models on multiple datasets to ensure generalizability across different domains. Comparative analyses consistently show that ensemble models outperform standalone algorithms in terms of accuracy, F1 score, and robustness against varied anomaly types. The FusionNet model builds on this foundation by integrating Random Forest, KNN, SVM, and MLP into a cohesive ensemble, benefiting from the diversity of learning mechanisms. The promising results of FusionNet in achieving high accuracy and precision reflect the growing consensus that combining heterogeneous algorithms can significantly enhance anomaly detection performance in practical, real-world applications such as healthcare and security.

Maryam Marshal et al. [6] The integration of Internet of Things (IoT) technology in healthcare has revolutionized patient monitoring by enabling continuous collection and real-time analysis of vital health data. However, this expansion also introduces significant cybersecurity challenges, including data breaches and privacy violations, which can severely impact sensitive healthcare information. Several studies have emphasized the importance of robust anomaly detection systems to protect IoT-enabled healthcare networks from cyber attacks. Machine learning techniques such as Random Forest, Adaptive Boosting, Logistic Regression, and Deep Neural Networks have gained widespread attention for their capability to identify abnormal network traffic patterns indicative of security threats. Prior research has utilized various datasets like NSL-KDD and CIC to evaluate the performance of these algorithms in detecting intrusions in IoT environments. Feature selection and dimensionality reduction methods have been highlighted as crucial steps to enhance model accuracy, reduce overfitting, and improve computational efficiency, which is critical for timely detection in healthcare scenarios. Ensemble methods, especially Random Forest, consistently outperform single classifiers due to their robustness and ability to handle imbalanced data. The CIC IoT dataset, with its diverse representation of 33 attack types grouped into seven categories, provides a comprehensive benchmark for developing realistic intrusion detection models tailored for IoT healthcare systems. Recent work has demonstrated that balancing class distributions and eliminating redundant features significantly boosts model performance. This study builds on these

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

foundations by applying advanced preprocessing and supervised learning models to the CIC dataset, confirming Random Forest's superior performance in both binary and multiclass classification tasks. The reduction in computational time achieved alongside high accuracy makes the approach practical for real-time IoT.

Mahmudal Hassan et al. [7] The rapid proliferation of Internet of Things (IoT) infrastructure across diverse domains has led to an increased focus on securing these systems from a variety of cyber threats. Attacks such as Denial of Service (DoS), Data Type Probing, Malicious Control, Malicious Operation, Scanning, Spying, and Wrong Setup pose significant risks to the reliability and safety of IoT environments. Detecting such anomalies and attacks in real-time remains a crucial challenge due to the resource constraints and heterogeneity of IoT devices. Machine learning (ML) techniques have become prominent tools in addressing this challenge by analyzing network behavior and classifying malicious traffic effectively. Common ML algorithms, including Logistic Regression (LR), Support Vector Machine (SVM), Decision Tree (DT), Random Forest (RF), and Artificial Neural Networks (ANN), have been widely applied in intrusion detection systems for IoT. Previous studies emphasize the importance of evaluating models not just on accuracy, but also on precision, recall, F1-score, and the Area Under the ROC Curve (AUC) to fully understand their effectiveness against imbalanced datasets typical in IoT attacks. Research indicates that while DT, RF, and ANN often achieve similar high accuracy rates, ensemble methods like Random Forest frequently outperform others in handling complex attack patterns due to their robustness and ability to reduce overfitting. The comparison of these models on diverse IoT attack types underlines Random Forest's superior balance of detection metrics, making it a preferred choice for anomaly detection in IoT systems. This study corroborates these findings by demonstrating that Random Forest, along with DT and ANN, can achieve near-perfect accuracy (99.4%) while maintaining better overall performance, thus contributing to more reliable and efficient IoT security frameworks.

Rajendra Kumar Dwivedi et al. [8] The rise of smart information systems, driven by sensor networks, has resulted in massive volumes of data being generated and stored in cloud environments for processing and analysis. However, sensor data can often contain anomalies caused by factors such as malicious intrusions, sensor malfunctions,

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

or challenging deployment conditions. Detecting these anomalies is vital, especially in sensitive domains like healthcare monitoring, environmental surveillance, and other IoT applications, where accurate and timely data interpretation is critical. Several anomaly detection techniques have been explored, with machine learning approaches gaining significant attention due to their ability to learn complex data patterns. Traditional methods such as Support Vector Machines (SVM) and Self-Organizing Maps (SOM) have been widely used for supervised anomaly detection, providing reasonable accuracy but sometimes limited by computational complexity or sensitivity to noisy data. This paper proposes a Gaussian Distribution-based Anomaly detection (GDA) scheme tailored for healthcare monitoring sensor clouds, integrating diverse body sensor data into a cloud platform. The utilization of the Gaussian statistical model enhances the detection precision and system throughput by modeling normal behavior effectively and distinguishing anomalies efficiently. Implemented in Python, the GDA approach achieves a high efficiency of 98%, demonstrating a notable improvement of 3% over SVM and 4% over SOM-based methods. This highlights the benefits of Gaussian-based statistical modeling in improving anomaly detection accuracy while maintaining computational efficiency, which is essential for real-time healthcare applications.

Monika Vishwakarma et al. [9] The increasing adoption of Internet of Things (IoT) technology has significantly transformed various sectors, raising critical concerns about security and privacy. Intrusion Detection Systems (IDS) have become essential tools to safeguard IoT networks by identifying malicious activities and distinguishing them from normal behavior. Various IDS approaches have been proposed, including supervised and unsupervised machine learning methods, to improve detection accuracy and reduce false alarms. This paper introduces a novel two-phase IDS tailored for IoT environments. The first phase categorizes data by types—nominal, integer, binary, and float—and employs different Naive Bayes classifier variants to perform initial classification. A majority voting mechanism consolidates these results to improve decision reliability. In the second phase, data identified as benign or normal undergo further scrutiny through an unsupervised elliptic envelope method to detect subtle anomalies. The system's effectiveness was validated on benchmark datasets including NSL-KDD, UNSW_NB15, and CIC-IDS2017. The results show

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

that the proposed hybrid approach achieves high accuracy—97% on NSL-KDD, 86.9% on UNSW_NB15, and 98.59% on CIC-IDS2017—outperforming several existing IDS methods. The integration of supervised and unsupervised techniques helps in balancing detection precision and reducing false positives. These findings underscore the importance of multi-phase and multi-method IDS frameworks for enhancing security in IoT systems. The paper contributes to the growing body of work seeking to protect IoT infrastructure from increasingly sophisticated cyber threats by leveraging data type-specific classification and anomaly detection.

AbdulWahib et al. [10] The Internet of Medical Things (IoMT) has revolutionized healthcare by enabling real-time monitoring through interconnected biosensors. However, the security challenges posed by the large volume of network traffic data, diverse cyber-attack patterns, and resource-constrained devices remain significant. The base paper proposes an explainable neural network (XNN) architecture targeting middlebox-based attacks in IoMT, achieving impressive classification accuracies of 99.7% and 99.4% on two distinct datasets. Their approach addresses Server-Side Includes (SSI) attacks and leverages flow-based network intrusion detection systems (NIDS) to improve detection throughput by eliminating packet RTT outliers. While these contributions are notable, the precision, recall, F1-score, and overall accuracy reported are marginally less comprehensive in terms of anomaly detection performance metrics. In contrast, the current study presents an Artificial Neural Network (ANN) model specifically optimized for the classification of IoT device states within the medical industry, achieving a uniformly high precision, recall, F1-score, and accuracy of 99.53%. This balanced performance across all key metrics demonstrates a more robust and reliable anomaly detection capability. Moreover, the proposed model efficiently handles diverse attack types with improved generalization and minimal false positives, which are critical in sensitive medical environments where false alarms can hinder timely interventions. By integrating feature selection and advanced training techniques tailored to medical IoT traffic characteristics, the present work surpasses existing methods in detection accuracy and operational efficiency. Thus, this research offers a more effective and scalable solution for securing IoMT infrastructures against evolving cyber threats.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

Souri et al. [11] The rapid advancement of sensor technologies has significantly contributed to the expansion of Internet of Things (IoT) applications, particularly in healthcare monitoring systems. The referenced paper presents an IoT-based student healthcare monitoring model designed to track students' physiological and behavioral health remotely, which is crucial for students living alone across dispersed locations. The model leverages IoT devices to continuously collect vital signs data, enabling real-time health monitoring. Machine learning techniques are employed to analyze the collected data and detect potential risks related to students' health changes. Among the algorithms tested, Support Vector Machine (SVM) demonstrated superior performance with an accuracy of 99.1%, outperforming Decision Tree, Random Forest, and Multilayer Perceptron (MLP) neural networks. This high accuracy indicates the model's robustness in accurately predicting physiological and behavioral anomalies in students. The study highlights the potential of integrating IoT with machine learning for efficient and proactive healthcare monitoring, ensuring timely intervention. Furthermore, the model's ability to maintain efficiency while handling continuous data streams emphasizes its suitability for real-world deployment. This approach also addresses the growing need for scalable healthcare solutions that can monitor large, geographically scattered populations effectively. Overall, the paper contributes valuable insights into applying IoT-enabled health monitoring combined with machine learning algorithms to improve student well-being.

Anurag Tiwari et al. [12] The integration of IoT and smart healthcare systems has revolutionized patient behavioral analysis, enabling more personalized and effective treatment approaches. Traditional healthcare faces significant challenges in monitoring patient behavior, especially for neurological, mental, and trauma-related conditions. Recent advancements in information technology, particularly IoT and cloud computing, have transformed healthcare by facilitating real-time data collection and remote monitoring through smart devices. These technologies allow continuous tracking of vital signs such as heart rate, body temperature, and environmental conditions, which are crucial for accurate diagnosis and patient management. The proposed smart healthcare system utilizes sensors like CO and CO₂ detectors alongside physiological monitors to gather comprehensive patient data. Artificial intelligence, including Artificial Neural Networks (ANN), enhances the accuracy and

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

efficiency of diagnosis and patient engagement by analyzing complex biomarker patterns. Experimental evaluations demonstrate minimal error rates across various sensor measurements, validating the system's reliability. Despite minor deviations caused by patient movement and sensor misplacement, the system maintains an acceptable error margin below 5%, ensuring dependable monitoring. Furthermore, data security measures restrict access to authorized personnel, safeguarding patient privacy. The system's capability to remotely provide real-time health status supports timely medical interventions. Overall, this study highlights the potential of IoT-driven smart healthcare architectures combined with AI to improve patient outcomes in medical environments. The approach offers a scalable, energy-efficient solution that can be adapted across diverse healthcare settings.

Romany Fouad Mansour et al. [13] Recent advancements in Internet of Things (IoT), cloud computing, and Artificial Intelligence (AI) have significantly transformed traditional healthcare into smart healthcare systems. The integration of IoT and AI offers innovative opportunities for improving disease diagnosis and patient management. Wearable devices and sensors facilitate continuous and seamless data acquisition, providing real-time physiological information crucial for accurate diagnosis. AI models, especially deep learning techniques, effectively analyze complex healthcare data to detect diseases early and with higher accuracy. The paper proposes a novel convergence of AI and IoT by introducing a Crow Search Optimization-based Cascaded Long Short-Term Memory (CSO-CLSTM) model for diagnosing heart disease and diabetes. The CSO algorithm optimizes the weights and biases of the CLSTM model, enhancing classification performance significantly. Additionally, the use of Isolation Forest (iForest) for outlier removal improves the quality and reliability of input data. Experimental results validate the model's effectiveness, achieving accuracies of 96.16% for heart disease and 97.26% for diabetes diagnosis. This demonstrates the potential of hybrid optimization and deep learning approaches in smart healthcare. The study highlights the importance of parameter tuning and data preprocessing in improving AI model outcomes. Such integrated AI-IoT systems can offer scalable, real-time, and precise diagnostic tools, supporting timely medical interventions. The approach is particularly promising for chronic disease management, where early detection is critical. Overall, this research

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

underscores the potential of AI and IoT convergence in revolutionizing healthcare delivery and improving patient outcomes.

Marcin Wozniak et al. [14] Health informatics has rapidly evolved as a crucial domain in modern healthcare, focusing on enhancing patient-centered care through advanced computational techniques. Computational intelligence, particularly deep learning, plays a vital role in developing secure and efficient decision support systems for automated diagnosis. The study introduces a novel Internet of Things (IoT) system that integrates a Bidirectional Long Short-Term Memory (BiLSTM) deep learning model with a Decision Tree classifier to improve diagnostic accuracy. Data preprocessing and balancing are critical steps to ensure reliable model training; thus, algorithms such as ADASYN and SMOTE-Tomek are employed to address class imbalance and enhance data quality. These techniques prevent bias and overfitting, enabling the model to generalize better on unseen data. The proposed system not only automates disease diagnosis based on patient questionnaire data but also facilitates secure document exchange between patients and healthcare providers, improving communication efficiency. Experimental results validate the model's performance, achieving an accuracy exceeding 96%, precision over 88%, and recall above 96%, demonstrating its robustness and reliability. The hybrid approach leveraging BiLSTM's ability to capture sequential dependencies and the Decision Tree's interpretability offers a powerful solution for healthcare diagnostics. This research highlights the importance of combining advanced deep learning models with traditional machine learning techniques for improved outcomes.

Iqra Yousaf et al. [15] Software plays a critical role across various healthcare processes, from appointment scheduling to patient treatment and care management. High-quality healthcare software systems, including hospital management systems, medical electronic systems, and middleware for medical devices, have been developed by vendors to support healthcare delivery. Recently, Internet of Things (IoT) medical devices have gained significant attention due to their ability to continuously monitor patients' health conditions, especially for brain-related diseases like Alzheimer's, Parkinson's, and traumatic brain injury. These IoT devices rely heavily on embedded software, whose complexity increases with the growing number of features and functionalities. However, software bugs in IoT medical devices pose

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

serious risks, including inaccurate health records, treatment delays, and in extreme cases, fatal consequences. Predicting the severity of such bugs is crucial given the critical nature of medical IoT systems. This research proposes a hybrid bug severity prediction model that combines Convolutional Neural Networks (CNN) with Harris Hawk Optimization (HHO) for hyperparameter tuning. The dataset used contains bug reports from healthcare systems and IoT medical devices, enabling thorough evaluation. The methodology involves preprocessing the textual dataset and extracting features suitable for the CNN embedding layer. The HHO algorithm optimizes critical hyperparameters such as batch size, learning rate, activation functions, optimizers, and kernel initializers before training. A 10-fold cross-validation approach validates the model's robustness. The hybrid CNN-HHO model achieved an impressive accuracy of 96.21%, demonstrating its effectiveness in predicting bug severity. This approach highlights the potential of combining deep learning with optimization techniques to improve software reliability in healthcare IoT devices. Such predictive models can significantly reduce risks associated with software failures, ensuring safer patient care and efficient medical device performance.

Dheyaaldin Alsalman et al. [16] Anomaly detection is essential in many critical fields such as cybersecurity, healthcare, and network monitoring, where timely and accurate identification of abnormal patterns can prevent severe consequences. Traditional machine learning algorithms like Support Vector Machine (SVM), K-Nearest Neighbors (KNN), and Random Forest (RF) have been extensively used for anomaly detection due to their interpretability and proven effectiveness. However, these individual models often struggle to capture the full complexity of diverse data distributions, which can lead to reduced detection accuracy. To address these challenges, ensemble learning techniques have been proposed, combining multiple classifiers to improve robustness and overall predictive performance. Recent studies have shown that ensemble models can leverage the complementary strengths of base learners to outperform single models. FusionNet, an innovative ensemble model, integrates Random Forest, KNN, SVM, and Multi-Layer Perceptron (MLP) to harness the unique advantages of each algorithm. This hybrid approach enhances detection accuracy, precision, recall, and F1 score across diverse datasets. Evaluations on two different datasets demonstrate FusionNet's superiority over traditional methods,

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

achieving accuracy rates as high as 98.5% and 99.5%. These results highlight the importance of combining heterogeneous algorithms to tackle the challenges of anomaly detection effectively. FusionNet's performance signifies its potential for real-world applications, especially in domains where accurate detection is vital. The model's success illustrates the growing trend toward sophisticated ensemble methods in anomaly detection research, reflecting ongoing advancements in machine learning applications.

Naim Shaik et al. [17] Predictive maintenance has become a vital research area for ensuring the reliability and efficiency of industrial systems, especially in critical infrastructure such as electric power plants. Machine learning techniques have been widely applied to analyze sensor data and predict equipment failures before they occur, reducing downtime and maintenance costs. Traditional models like K-Nearest Neighbors (KNN) and Naive Bayes (NB) have been popular for their simplicity and probabilistic interpretability, though they may have limitations in capturing complex data patterns. Deep learning models, including Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), have demonstrated superior performance in various predictive maintenance tasks due to their ability to extract spatial and temporal features from sensor data. CNNs are particularly effective in recognizing spatial correlations, leading to higher accuracy in fault detection, as supported by several recent studies. Meanwhile, RNNs excel at modeling time-dependent sequences, making them suitable for analyzing time-series data in maintenance scenarios. Comparative research has consistently shown that deep learning models outperform classical algorithms like KNN and NB, albeit with increased computational complexity. This study corroborates these findings by achieving the highest accuracy with CNN (96.5%) followed by RNN (92.2%), KNN (89.7%), and NB (85.4%). The research emphasizes the importance of selecting appropriate models based on the nature of the data and operational needs. Moreover, it highlights the potential of hyperparameter tuning and model adaptability to enhance predictive capabilities. The insights gained here provide a foundation for developing robust maintenance strategies in small-scale power systems, contributing to the broader field of industrial AI applications.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

Himanshu sinha et al. [18] Time series novelty or anomaly detection is an important and challenging area in data mining, focusing on identifying unusual patterns or deviations in sequential data. Its relevance has grown rapidly due to applications across fields like finance, healthcare, and network security. Traditional statistical models such as ARIMA have been widely used for forecasting and anomaly detection due to their ability to model temporal dependencies. However, with increasing data complexity, machine learning (ML) techniques have shown promising improvements in detecting novelties in time series data. Recent studies have demonstrated the effectiveness of ensemble models like Random Forest Regressor in handling noisy and high-dimensional data. These models outperform classical approaches by capturing complex relationships and interactions among features. Data preprocessing, including handling missing values and feature engineering, is critical for improving model accuracy in anomaly detection tasks. Visualization techniques have also been applied to better understand temporal patterns and assist in identifying outliers. Comparative analysis shows that Random Forest consistently achieves lower error metrics, such as MAE, RMSE, and MSE, than other models including ARIMA and Decision Tree Regressors. The superior performance of Random Forest highlights its robustness and adaptability to various time series datasets. Meanwhile, Decision Tree models often suffer from overfitting and higher error rates, making them less suitable for precise novelty detection. This research underlines the importance of careful model selection and tuning in time series anomaly detection. The findings contribute valuable insights for applying ML techniques to real-world time series datasets, such as those from online platforms like Stack Overflow. Overall, this work emphasizes that hybrid approaches combining classical and machine learning methods may further enhance detection accuracy in future studies.

Gifty Acquah et al. [19] Anomaly detection in smart grid systems has gained critical importance due to the increasing frequency and sophistication of cyberattacks. The fuzzy and dynamic characteristics of these cyber threats pose significant challenges for accurate detection, often resulting in abnormal system predictions. With the transformation of traditional power grids into integrated cyber-physical communication networks, vulnerabilities have increased, exposing systems to attacks like the Ukraine power system cyberattack (2015), Iran Aramco attack (2017), and

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

New York smart grid attack (2018). These incidents underscore the severe impact of cyberattacks on infrastructure, economy, and public safety. Given the large scale and complexity of smart grids, manual monitoring is impractical, driving the need for automated anomaly detection solutions. Machine learning (ML) methods have emerged as powerful tools for identifying suspicious activities within smart grid communication networks. ML techniques enable the transition from simple secure communication frameworks to intelligent security systems capable of real-time threat identification. Several supervised ML models, including decision trees, support vector machines, and neural networks, have been explored for intrusion detection in smart grids. However, each model has limitations related to false positives, detection latency, or sensitivity to novel attacks. Recent research highlights the benefits of hybrid approaches that integrate multiple ML models into ensemble systems, improving detection accuracy and reducing errors. These integrated Intrusion Detection Systems (IDS) can complement individual model weaknesses, providing robust protection against a variety of cyber threats. Furthermore, the complexity of smart grid networks necessitates adaptive and scalable ML algorithms to manage evolving attack strategies. Studies also emphasize the importance of feature selection and data preprocessing in enhancing ML performance for anomaly detection. Real-world deployments reveal that combining ML with domain-specific knowledge yields more reliable results. This dissertation's focus on multi-model integration aligns with current trends aiming to bolster the cybersecurity of smart grids. Overall, ML-driven IDS represent a promising direction to safeguard smart grid infrastructure against increasingly sophisticated cyber threats.

Adisu Mulu Seba et al. [20] Internet of Things (IoT) ecosystems largely depend on the accuracy of sensor data, which can be compromised by environmental disturbances and electrical noise. Resource-limited sensors are prone to faults, producing erroneous measurements that may lead to severe consequences, especially in critical applications. Traditional research in this area has predominantly focused on fault detection, which is a reactive approach identifying faults only after they have impacted the system. Such delayed responses can result in negative outcomes, highlighting the need for proactive fault management techniques. Recent studies have explored forecasting-based approaches that predict sensor measurements in advance,

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

enabling earlier intervention. Hybrid deep learning models, particularly those combining convolutional neural networks (CNN) with recurrent architectures like long short-term memory (LSTM), have demonstrated promise in time series forecasting of sensor data. Integrating CNN with LSTM captures both spatial and temporal dependencies effectively, enhancing prediction accuracy. To extend beyond forecasting, researchers have investigated fault classification models that categorize sensor anomalies into different fault types, such as bias, drift, or random faults. Multi-layer perceptron (MLP) networks and hybrid CNN-MLP architectures have been employed to improve classification robustness. The use of fault-injected annotated datasets, like the Intel Lab raw dataset, facilitates comprehensive training and evaluation of such models. Cross-validation techniques have been adopted to ensure generalizability across time series splits. Studies emphasize the significance of a two-stage approach combining forecasting and classification to anticipate faults before they manifest, enabling proactive maintenance.

Ghazal Ghajari et al. [21] networks has introduced significant challenges in ensuring robust network security. Traditional intrusion detection systems (IDSs) often struggle to efficiently process high-dimensional and complex network data, limiting their effectiveness against sophisticated cyberattacks. Recent research has explored novel computational paradigms to overcome these limitations, with hyperdimensional computing (HDC) emerging as a promising approach. HDC is inspired by brain-like processing and offers efficient handling of large-scale data through high-dimensional vector representations. Several studies have demonstrated the potential of HDC in various domains requiring fast and scalable data analysis. The application of HDC to network anomaly detection is gaining traction due to its ability to identify both known and novel attack patterns. Specifically, the NSL-KDD dataset has become a standard benchmark for evaluating IDS models in IoT and general network security contexts. Comparative analyses with traditional machine learning models reveal that HDC-based methods can achieve competitive or superior accuracy while maintaining computational efficiency. The capability of HDC to generalize across varying data distributions makes it suitable for the dynamic and evolving nature of IoT network traffic. This approach reduces false positives and enhances real-time detection capabilities, addressing the pressing needs of modern cybersecurity systems.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

Additionally, HDC's lightweight computational requirements support deployment in resource-constrained IoT environments. Current studies underscore the value of integrating HDC into IDS frameworks to improve detection rates without compromising speed. Overall, hyperdimensional computing presents a novel and efficient paradigm for enhancing network anomaly detection in IoT, contributing to the advancement of intelligent and secure cybersecurity solutions.

Bayu Adhi Tama et al. [22] Intrusion Detection Systems (IDSs) are crucial for identifying and preventing malicious activities in computer networks. Anomaly-based IDSs rely on classification models trained with historical data to detect unknown attacks. Feature selection plays a vital role in enhancing IDS accuracy and efficiency by reducing dimensionality. Hybrid feature selection techniques combining Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), and Genetic Algorithms (GA) have been shown to select optimal features, improving model performance on datasets like NSL-KDD and UNSW-NB15. Ensemble learning methods such as Rotation Forest and Bagging have been successfully applied to improve robustness and detection accuracy. The proposed approach uses a two-level classifier ensemble with these meta-learners, effectively combining strengths of multiple classifiers. Experimental results on the NSL-KDD dataset demonstrate an accuracy of 85.8%, sensitivity of 86.8%, and detection rate of 88.0%, outperforming several recent techniques. On the UNSW-NB15 dataset, the model also shows significant improvement over state-of-the-art methods. A two-step statistical significance test was conducted to validate these results, adding robustness to the findings. This research highlights the benefits of integrating hybrid feature selection with ensemble classifiers to enhance IDS performance, making it a promising strategy for combating evolving cyber threats.

Martha et al. [23] The Industrial Internet of Things (IIoT) has revolutionized traditional industrial processes by enabling enhanced connectivity, real-time monitoring, and proactive maintenance. The integration of advanced sensors and communication technologies facilitates increased operational efficiency but also raises concerns about system dependability and security. Anomaly detection in IIoT systems has become critical to ensure safety and uninterrupted operations. Prior research has explored various machine learning and deep learning techniques for detecting faults

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

and cyberattacks in industrial environments. Unsupervised models are particularly useful in monitoring system behavior continuously without requiring labeled data. However, effective classification of detected anomalies remains a challenge, necessitating hybrid frameworks that combine unsupervised detection with supervised classification. This approach helps in distinguishing between different types of anomalies, such as system failures or malicious attacks. The proposed IIoT Anomaly Classification Framework aligns with recent trends emphasizing scalable and adaptable solutions suited for diverse industrial settings. Evaluation through cross-validation using realistic IIoT datasets demonstrates strong precision, recall, and F1-score, highlighting the model's robustness. Such results reinforce the importance of combining anomaly detection and classification to improve system resilience. Furthermore, this research contributes to ongoing efforts in strengthening IIoT security and reliability, laying groundwork for future enhancements in anomaly management and industrial process optimization.

G Logeswari et al. [24] The proliferation of Internet of Things (IoT) devices has introduced significant security challenges, particularly for Intrusion Detection Systems (IDS) that must process vast, heterogeneous data streams. Traditional IDS approaches often struggle with complex attack patterns and high-dimensional data. Recent research highlights the importance of integrating advanced optimization and deep learning techniques to enhance detection capabilities. Quantum-Inspired Particle Swarm Optimization (QIPSO) has shown promise in feature selection by efficiently narrowing down relevant attributes in large datasets. Adaptive Neuro-Fuzzy Inference Systems (ANFIS) add value by managing uncertainty and imprecision inherent in IoT traffic. Capsule Networks (CapsNets), known for their ability to capture spatial hierarchies, and Attention-Augmented RNNs, adept at modeling temporal dependencies, are increasingly used in multi-stage classification pipelines. The combination of these models offers a robust framework for detecting both known and unknown threats. The proposed hybrid IDS framework leverages QIPSO-ANFIS for optimal feature extraction and integrates CapsNets with attention-RNNs for accurate classification. Evaluation on TON-IoT and BOT-IoT datasets demonstrates the model's superior accuracy and generalization ability. The approach significantly improves precision and F-measure, outperforming traditional methods. This study

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

contributes a novel, adaptive IDS tailored for real-time intrusion detection in dynamic IoT ecosystems, bridging a crucial gap in existing cybersecurity solutions.

Ntayagabiri et al. [25] The rapid expansion of IoT devices has led to a surge in security threats, necessitating advanced intrusion detection techniques. Traditional detection systems face challenges in handling the complexity and scale of IoT-generated data. To address this, recent research focuses on evaluating machine learning algorithms for attack classification. This study conducts a comparative analysis of ten supervised learning models—Naive Bayes, ANN, Logistic Regression, k-NN, XGBoost, Random Forest, LightGBM, GRU, LSTM, and CNN—on the CICIoT2023 dataset. The dataset includes data from 105 devices and 33 attack types, offering comprehensive evaluation scenarios. Ensemble models such as Random Forest and XGBoost outperform others in terms of accuracy and precision, with RF achieving 99.29% accuracy and 82.30% precision. While deep learning models like CNN also perform well (98.33% accuracy), precision and recall vary due to class imbalance. The confusion matrix analysis reveals algorithm-specific strengths and weaknesses in detecting certain attack types. Notably, the recall metric, often overlooked, proves vital in minimizing the risk of undetected threats. For instance, RF's recall of 72.19% outperforms CNN's 64.72%, underscoring the need for balanced detection strategies. This work emphasizes that while high accuracy is essential, practical deployment requires algorithms that balance precision and recall. The findings contribute to the development of context-aware, effective IDS solutions tailored for complex IoT environments.

Sana Abdelaziz et al. [26] With the growing integration of IoT devices in smart environments, device classification has become essential for ensuring secure and efficient system operations. Accurate identification of device types supports improved device management, network integrity, and security monitoring. Recent studies have explored machine learning approaches to classify IoT devices based on network traffic data. This work presents a comparative analysis of two powerful ensemble classifiers—Gradient Boosting (GB) and Random Forest (RF)—on a dataset of 1,900 smart home devices categorized into ten functional groups. Both models were evaluated using key metrics including accuracy, precision, recall, F1-score, Matthews Correlation Coefficient (MCC), and Area Under the Curve (AUC), supported by 20-

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

fold cross-validation. Gradient Boosting exhibited superior performance with a precision of 92%, recall of 90%, and an F1-score of 91%, indicating robust predictive power. Random Forest, while slightly trailing in precision (89%), recall (87%), and F1-score (88%), achieved a higher AUC of 0.94, suggesting better discrimination capability in certain classes. ROC curve analysis further revealed the true-positive vs. false-positive trade-offs. Confusion matrices showed misclassifications in classes with overlapping network behaviors. Both models highlighted the need for refined feature engineering to improve category separation. The study confirms the viability of advanced ensemble methods for enhancing IoT device classification in smart home systems. Overall, this research contributes to developing secure and context-aware IoT frameworks through intelligent traffic-based classification techniques.

Fransico et al. [27] The modern sedentary lifestyle, primarily driven by increased computer usage for both work and leisure, has resulted in a significant rise in musculoskeletal disorders. Extended sitting durations, especially in improper postures, contribute to chronic back pain and other health complications. Various studies have explored ergonomic interventions and wearable technologies for posture monitoring, yet most solutions are either expensive or cumbersome. IoT-based posture detection systems present a promising alternative due to their low cost and real-time monitoring capabilities. Force Sensitive Resistors (FSRs) have been effectively used in seat-based configurations to detect pressure distribution patterns. Several works have highlighted the potential of Artificial Neural Networks (ANNs) in classifying physical postures due to their high adaptability and learning efficiency. This particular study integrates FSRs with an ANN model to classify sitting postures into seven categories, including a neutral and six incorrect ones. Data collection from 12 users under controlled conditions enhanced the dataset diversity. The hold-out validation technique was used to prevent overfitting during the training phase. The best-performing ANN architecture used two hidden layers with 128 neurons each. It achieved an average accuracy of 81%, indicating promising reliability. This performance affirms the ANN's capacity to differentiate posture patterns based on seat pressure maps. Compared to vision-based systems, this approach reduces privacy concerns and setup complexity. Prior works have used more sensors or complex configurations; however, this study demonstrates effectiveness with minimal hardware. The reduced sensor

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

count also implies lower energy consumption and higher feasibility for practical deployment. The study builds on existing literature by proving high classification accuracy without compromising system simplicity.

Ke Qi et al. [28] proposes a multilayer machine learning framework for secure and intelligent health monitoring in IoT-based smart healthcare systems. The proposed model integrates an IoT-sensor environment with edge, fog, and cloud computing layers to ensure end-to-end health data collection, processing, and storage. To classify patient states, the model employs a three-layer Artificial Neural Network (ANN), optimized to operate efficiently across decentralized nodes. A key focus of the research is on ensuring both data security and classification accuracy, given the sensitivity of medical data. The ANN model is trained using a real-world dataset composed of physiological and behavioral health parameters. The multilayer deployment enhances not only computation efficiency but also minimizes latency and energy consumption across the network. Performance evaluation is conducted using metrics such as accuracy, precision, recall, F1-score, and execution time. The ANN model achieved 91.34% accuracy, 92.18% precision, and 90.56% recall, demonstrating a reliable balance between detection quality and resource utilization. The paper also includes a comparative analysis with other classifiers like SVM, Decision Trees, and Naive Bayes, where ANN consistently outperforms alternatives in terms of classification and scalability. However, the authors note that the ANN model struggled with overlapping feature classes and data imbalance, which are typical challenges in IoT-based health monitoring. Additionally, the system's modular design enables future integration with blockchain or federated learning for improved data privacy. Overall, this study contributes significantly to the literature by addressing real-time monitoring, data security, and intelligent health status classification through ANN in IoT-medical applications.

Tanzila Saba et al. [29] The increasing deployment of Internet of Things (IoT) devices across various domains has introduced new vectors for cyber threats, making security a pressing concern. This study addresses the critical challenge of securing IoT environments through an intelligent anomaly-based Intrusion Detection System (IDS). It proposes a Convolutional Neural Network (CNN)-based model for detecting abnormal traffic and potential intrusions. Traditional security approaches have shown

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

limitations in dynamic and heterogeneous IoT networks, which require adaptive and scalable solutions. Machine learning has gained prominence, but deep learning techniques, particularly CNNs, offer superior performance due to their ability to automatically extract features from raw input. The authors trained and evaluated their CNN model using two benchmark datasets—NID and BoT-IoT. On the NID dataset, the model achieved an outstanding accuracy of 99.51%, while on the BoT-IoT dataset, it reached 92.85% accuracy, indicating strong generalizability across datasets. The proposed IDS model effectively distinguishes normal from anomalous traffic patterns by learning spatial-temporal relationships in packet flow data. The study emphasizes the CNN's capacity to analyze full IoT network traffic without the need for handcrafted features, improving detection speed and reliability. However, the paper notes some limitations related to imbalanced class distributions and overfitting risks in deep learning models. These challenges point to the need for further optimization in preprocessing and architecture tuning. This work reinforces the value of CNNs in IoT security systems and contributes to the growing field of AI-driven anomaly detection. It demonstrates that deep learning, when properly trained, can significantly outperform traditional rule-based or statistical IDS solutions, paving the way for autonomous and secure IoT deployments.

Paulo Angelo et al. [30] Intrusion Detection Systems (IDS) remain vital in safeguarding cyberspace against evolving threats. This study explores anomaly-based IDS approaches, which define “normal” system behavior and flag deviations as potential intrusions. The authors propose an adaptive framework that uses genetic algorithms (GA) for dynamic feature selection and parameter optimization in anomaly detection tasks. The core idea involves profiling—establishing a baseline of normal activity—and adapting detection strategies based on evolving behaviors. Two novel anomaly detection techniques are introduced: one relies on basic statistical analysis, and the other utilizes a projected clustering method to capture complex patterns in traffic data. This adaptive system not only selects the most relevant features but also aligns with system and user constraints, including available computational resources and operator-defined policies. The approach was validated using the CICIDS2017 dataset, a comprehensive benchmark for modern network traffic, ensuring realistic and complex evaluation scenarios. The proposed system achieved a detection rate of

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

92.85% and a false positive rate of just 0.69%, demonstrating high accuracy with minimal noise. The iterative nature of the model ensures that it remains responsive to newly emerging attacks, enhancing long-term system resilience. By integrating genetic algorithms with anomaly-based profiling and clustering, the study presents a flexible and efficient methodology for real-world intrusion detection applications. Its adaptability and high detection capability make it suitable for deployment in dynamic IoT and enterprise environments. This research contributes to the broader field by combining bio-inspired optimization techniques with unsupervised and semi-supervised learning, highlighting the potential of hybrid methods in enhancing the precision and robustness of cybersecurity solutions.

Khan et al. [31] The integration of IoT in healthcare has greatly enhanced patient monitoring and service efficiency. However, challenges like data security, interoperability, and ethical concerns still limit its full potential. IoT sensors continuously collect patient data and send it to central servers for analysis. Machine learning algorithms at the server end assist in early diagnosis and trigger alerts when abnormal health patterns are detected. Despite these benefits, IoT systems in healthcare are prone to various cyberattacks, risking patient data and system integrity. To address this, a study employed the CIC IoT dataset, which includes 33 IoT attack types grouped into seven categories. The dataset was cleaned and balanced to avoid model bias. Multiple supervised learning techniques, including Random Forest, AdaBoost, Logistic Regression, Perceptron, and Deep Neural Networks, were used to classify the attack types. Feature selection and dimensionality reduction were applied to enhance model performance and speed. Random Forest achieved the best results in both binary and multiclass scenarios. It maintained approximately 92% accuracy despite noisy data. The model also showed improved processing speed, essential for real-time threat detection in healthcare IoT systems.

Olwale et al. [32] The Internet of Healthcare Things (IoHT) is a growing field revolutionizing patient monitoring and health management through interconnected smart devices. However, its dependence on wireless internet connectivity exposes it to serious cybersecurity risks, raising concerns about data privacy and security. Recent

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

studies highlight the importance of leveraging Artificial Intelligence (AI) to detect and mitigate such vulnerabilities. With the continuous evolution of medical IT systems, protecting sensitive data collected by IoT sensors has become crucial. Researchers have turned to benchmark datasets like TON_IoT, Edge_IIoT, and UNSW-NB15 to evaluate AI models for security applications. These models were assessed for their ability to predict and detect threats effectively. To enhance data security, blockchain integration, specifically IPFS technology, was applied for decentralized storage. The Support Vector Machine (SVM) model showed the highest performance, achieving 100% accuracy on the TON_IoT dataset. Edge_IIoT and UNSW-NB15 datasets also showed promising results, with 98% and 89% accuracy, respectively. The study demonstrates how combining AI and blockchain can safeguard healthcare systems. It provides a foundational approach for ensuring data confidentiality and integrity. These findings offer a valuable direction for future research in the secure deployment of IoHT systems.

Ioannou et al. [33] With the rapid growth of IoT devices, especially in healthcare, securing sensitive data has become a pressing issue. Traditional cloud-based data analysis methods introduce delays and compromise privacy. To tackle this, a power-efficient Intrusion Detection System (IDS) is proposed for Medical IoT (MIoT) networks, structured into three stages. First, machine learning techniques are applied to classify known attacks like MitM and DDoS, enhancing threat detection and reporting. Second, anomaly detection is used to identify unknown threats, with the model retrained whenever new anomalies are found. Third, Federated Learning (FL) is employed to update the central model securely without sharing raw data, preserving user privacy. The Enhanced Random Forest model showed exceptional accuracy of 99.98% for attack classification. For anomaly detection, the One-Class SVM achieved 99.7% accuracy, making it reliable for identifying new threats. FL ensures efficient, private updates to the central system. This architecture was tested on real MIoT setups, including a Raspberry Pi gateway, confirming its reliability and low energy usage. Future work will aim to improve scalability and efficiency across wider MIoT deployments.

Sharma et al. [34] Securing Internet of Things (IoT) devices is becoming increasingly vital due to the vast number of interconnected devices handling sensitive information.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

IoT security focuses on preventing unauthorized access and ensuring the safe transmission of data across networks. Traditional machine learning (ML) algorithms are commonly used for anomaly detection, but they often fall short in identifying sophisticated intrusion attempts. To address this limitation, a novel approach called Stacked Long Short-Term Memory with Willow Catkin Optimization (SLSTM-WCO) has been introduced. This method enhances detection accuracy by learning complex data patterns using deep learning techniques. The SLSTM model effectively identifies irregularities, and the WCO algorithm fine-tunes it for better performance. Regularization techniques are used to improve generalization and reduce overfitting. This approach was tested on multiple benchmark datasets like BoT-IoT, IoT-23, and MQTT-based datasets. The proposed model achieved a notable accuracy of 99.49%, outperforming existing solutions. These results demonstrate its ability to significantly enhance anomaly detection in IoT systems. Overall, this work contributes to more reliable and secure IoT network monitoring.

Mathivanan et al. [35] With the growing need for continuous health tracking, remote patient monitoring (RPM) using IoT has become a crucial area of research. This study proposes an ensemble deep learning model combining Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks to enhance the accuracy and efficiency of RPM systems. The goal is to detect early signs of health issues by analyzing real-time physiological data collected via wearable IoT devices. CNNs are utilized to extract spatial features, while LSTMs capture temporal patterns, making the model highly effective in understanding health data trends. The proposed Remote Patient Monitor Model (RPMM) accurately tracks key health indicators such as heart rate, oxygen levels, blood pressure, temperature, sleep quality, and medication adherence. This hybrid model achieved a strong accuracy of 97.5%, proving its capability in identifying anomalies and supporting timely interventions. Its robustness was validated using diverse healthcare datasets. The approach improves the reliability of patient monitoring and supports proactive healthcare management. Overall, this research demonstrates how combining spatial and temporal deep learning techniques enhances the quality of patient care and reduces the load on healthcare systems.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

Vaisakhkrishnan et al. [36] The rapid adoption of the Internet of Medical Things (IoMT) has revolutionized healthcare by enabling continuous monitoring and data exchange through interconnected medical devices. However, this connectivity introduces significant cybersecurity threats that put both patient safety and data privacy at risk. This study focuses on enhancing IoMT security using advanced deep learning techniques for real-time threat detection and prevention. It addresses major cyberattacks such as backdoors, DDoS, MITM, ransomware, and SQL injections that could disrupt critical medical operations. A deep learning-based intrusion detection system is proposed to monitor the IoMT network and identify suspicious behavior. The research evaluates the performance of multiple models including CNN, Autoencoders, Transformers, and LSTM networks. Among them, the LSTM model optimized with the Adam optimizer (Adam-LSTM) achieved the highest performance, with 97% accuracy and strong precision, recall, and F1 scores. The study proves the effectiveness of this approach in securing IoMT systems against complex attacks. Comparative analysis further confirms its superiority over existing methods. This work lays a strong foundation for future developments in medical IoT cybersecurity. It also encourages the adoption of intelligent and safe digital healthcare infrastructures.

Prova et al. [37] Healthcare fraud is a serious issue in the United States, causing financial losses estimated in the tens of billions annually. These fraudulent activities range from billing for services not rendered to manipulating codes for higher reimbursements and illegal kickback schemes. In response to this challenge, the study explores the use of machine learning (ML) models to detect healthcare fraud effectively. Using a large dataset of over 550,000 inpatient and outpatient claims, integrated with beneficiary details, several ML models were applied, including Random Forest, XGBoost, SVM, Isolation Forest, deep learning, and a Stacking Ensemble method. Performance was assessed using metrics such as accuracy, precision, recall, F1 score, and ROC AUC. The Stacking Ensemble model stood out, achieving 92.79% accuracy and a high ROC AUC of 96.95%. To enhance model transparency, SHAP value analysis was used to explain predictions and highlight key features. The study also introduces a real-time fraud detection pipeline along with an automated retraining framework. This ensures that the system evolves with changing

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

fraud patterns. Overall, the research offers a robust and adaptive approach to mitigating healthcare fraud through intelligent ML systems.

Shakhovska et al. [38] Accurate prediction of medical insurance costs is a critical aspect of financial risk management in healthcare. This study introduces three novel ensemble models—boosting, bagging, and stacking—to enhance the prediction accuracy of individual insurance expenses. Using an open dataset, the paper applies feature selection techniques like the Pearson correlation coefficient and the Boruta algorithm to identify the most relevant features. Ensemble methods such as bagged CART, Random Forest, and boosting with regression trees and stochastic gradient descent were implemented and compared. Among the three, stacking outperformed others by combining various base models like KNN, SVM, regression trees, linear regression, and gradient boosting, with a Random Forest meta-learner using 100 trees. While bagging methods showed limitations in generalization, boosting and stacking provided significantly better results. The stacking model achieved a Root Mean Squared Error (RMSE) of 3173.213, outperforming all individual base learners. Its RMSE score was 1.47 times better than the best-performing single model, SVR. This research highlights how ensemble methods, especially stacking, can significantly improve the precision of cost prediction models. The findings support the broader use of AI in economic decision-making within healthcare, offering both cost savings and improved planning.

Duman et al. [39] With the widespread adoption of digital health records, healthcare systems are generating vast amounts of electronic medical data. While this brings numerous advantages, it also leads to challenges like rising costs and data management complexities. One effective approach to mitigate financial strain is the detection of healthcare fraud. This study explores the use of machine learning techniques, particularly focusing on XGBoost, an efficient gradient-boosted decision tree model, for fraud detection. Other supervised algorithms such as Random Forest, Logistic Regression, and Decision Trees were also evaluated. The Medicare Part B dataset was enriched by labeling fraud cases using the List of Excluded Individuals/Entities (LEIE) database. This allowed the use of supervised learning models for accurate fraud classification. Experimental results showed that XGBoost significantly outperformed other traditional models in terms of accuracy and

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

efficiency. The study demonstrates the potential of integrating robust ML models for real-world applications in digital healthcare systems. By detecting fraud more effectively, these models can help reduce operational costs and improve the overall integrity of healthcare data systems

Mohammad et al. [40] Blockchain (BC) has emerged as a transformative technology across multiple industries, including healthcare, where it enhances data transparency and patient control over medical records. Despite its potential, integrating blockchain into healthcare systems presents challenges, particularly in secure data storage and privacy protection. The rise of sophisticated attacks on various BC components—such as nodes, smart contracts (SCs), consensus protocols, and wallets—has raised serious security concerns. Fraudulent data insertion, in particular, threatens the integrity and reliability of the blockchain. This study addresses the need for robust security by proposing a two-stage system that leverages machine learning (ML) to detect fraudulent activities. First, it filters abnormal sensor data before it enters the BC. Second, it analyzes transactions, storing legitimate ones and flagging suspicious ones as novel attacks. Six ML models—Logistic Regression, Decision Tree, KNN, Naive Bayes, SVM, and Random Forest—were evaluated using two benchmark datasets. Among them, the Random Forest algorithm delivered the best performance in accuracy, execution time, and scalability. The proposed framework demonstrates strong potential in safeguarding blockchain-based healthcare applications from evolving security threats. Its adaptability and high detection capabilities make it a suitable solution for future secure medical data systems.

Johnson et al. [41] Detecting fraudulent healthcare providers through automated techniques can lead to significant cost savings and improved care quality. This study introduces a data-centric machine learning approach for healthcare fraud detection using Medicare claims data. Researchers utilized publicly available datasets from the Centers for Medicare & Medicaid Services (CMS), specifically spanning 2013–2019 and covering Medicare Part B, Part D, and DMEPOS claims. Nine large-scale, labeled datasets were created, each tailored for supervised learning. A detailed review of the data preparation steps and an enhanced data labeling method were presented. To improve prediction performance, the datasets were enriched with up to 58 new provider-specific features. The study also addressed a critical model evaluation

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

issue—target leakage—by introducing an adjusted cross-validation method for more reliable performance assessment. Models such as Extreme Gradient Boosting (XGBoost) and Random Forest were tested using diverse metrics and confidence intervals. Findings revealed that the enriched datasets outperformed the original Medicare datasets widely used in previous research. The results underscore the effectiveness of a data-centric ML workflow. This research provides a robust foundation for future fraud detection models and emphasizes the importance of data preparation in healthcare ML applications.

Sun et al. [42] Intrusion detection in smart healthcare applications is essential to protect patient data and system integrity. This study proposes a hybrid approach combining Particle Swarm Optimization (PSO) and AdaBoost algorithms to detect malware threats in medical IoT environments. Using the NSL-KDD dataset with over 125,000 instances and 41 features, the research first applies PSO for feature selection, narrowing down to 12 crucial attributes. The optimized dataset is then used to classify major attack types such as DoS, U2R, R2L, and Probe. AdaBoost emerged as the most effective classifier, achieving a high recall score of 0.966667, confirming its strength in identifying intrusions. The combined PSO-AdaBoost model demonstrated excellent accuracy, precision, and recall, outperforming conventional methods. The results indicate that integrating such ML-based Intrusion Detection Systems (IDS) into smart health applications can enhance data security and patient safety. This framework supports real-time threat monitoring in the Internet of Medical Things (IoMT) ecosystem. Additionally, it offers a scalable, cost-effective solution to counter evolving cyber threats in healthcare. The study emphasizes the importance of robust IDS in building secure digital health infrastructures.

Adeyinin et al. [43] The Internet of Medical Things (IoMT) integrates connected medical devices into public healthcare infrastructure, enabling real-time communication through wireless systems. IoMT facilitates smart interactions between machines, enhancing the capabilities of modern healthcare systems. This technology transforms regular medical tools into intelligent, networked systems using wearable body sensor networks (WBSNs) for health monitoring. While these sensors can detect anomalies and aid early diagnosis, their use in everyday clinical practice is still not widespread. The major challenges in adopting IoMT include data security,

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

authentication, and seamless information exchange. To address this, the study proposes a smart healthcare monitoring system architecture using IoMT and WBSNs. The system incorporates ensemble tree-based learning algorithms to identify health patterns and predict potential risks. It provides real-time alerts and suggestions to medical staff based on patient data trends. This proactive approach enables timely intervention and improves patient care. The method aims to reduce response times and increase the reliability of remote healthcare systems. The integration of such intelligent systems has shown promise in enhancing overall health outcomes.

Rayan et al. [44] The integration of big data in healthcare is rapidly advancing, with emerging innovations enhancing bioinformatics and health research. Modern devices such as smartphones, wearable sensors, and IoT-based systems are constantly generating vast volumes of health data from individuals, professionals, and institutions. This data, when effectively harnessed, can be instrumental in diagnosing and treating various diseases. A significant challenge lies in identifying, collecting, analyzing, and distributing this information efficiently for early detection of risk factors and proactive care. Mobile health (m-health) technologies have shown promise in managing chronic illnesses by facilitating real-time health monitoring. Smartphone applications now assist patients in tracking daily health metrics, and these tools are increasingly integrated into e-health and telemedicine solutions. The Internet of Things (IoT) further strengthens this ecosystem by enabling continuous communication between devices and healthcare systems. However, issues like data privacy and cybersecurity remain key concerns and need collaboration with policymakers. The study investigates the role of IoT and m-health in improving healthcare delivery and outlines innovative computational techniques to support this integration. Additionally, a novel model for diabetes self-management is proposed, demonstrating practical applications of these technologies in personalized care.

Ghubaish et al. [45] The surge in microcomputing, compact hardware manufacturing, and machine-to-machine (M2M) communications has paved the way for advanced IoT applications across industries, notably in healthcare. This evolution led to the emergence of the Internet of Medical Things (IoMT), which facilitates remote monitoring of patients, particularly those with chronic conditions. IoMT systems enhance emergency responsiveness by enabling timely diagnoses. However, despite

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

their benefits, the security of data within IoMT environments remains a significant concern. This paper presents a comprehensive review of current security methods applied during the data lifecycle—collection, transmission, and storage—in IoMT systems. It identifies various vulnerabilities, including physical and network-based attacks, and highlights a key gap: existing techniques often fail to address the full spectrum of threats. To bridge this gap, the study proposes a unified security framework that integrates multiple protection mechanisms. This proposed model ensures compliance with core IoMT security requirements and offers resilience against a wide range of known attack vectors. Ultimately, the framework aims to strengthen trust and encourage broader adoption of IoMT in clinical settings.

Ghummadi et al. [46] Healthcare data holds immense value as it often includes critical information related to human survival and well-being. Analyzing such data is essential, given its potential to save lives and enhance the quality of healthcare services. The emergence of the Internet of Things (IoT) has significantly transformed modern healthcare systems, enabling more efficient monitoring and management. IoT technologies offer remarkable promise in delivering proactive and personalized medical solutions. This work focuses on the application of proactive healthcare analytics for the early prevention of cardiac diseases. Anomaly detection is emphasized as a key component in these analytics, aiming to identify irregular health events with high accuracy. One of the main challenges is detecting anomalies under conditions of high noise, where the signal-to-noise ratio is low. Reducing false negatives in such scenarios is crucial to ensure timely medical interventions. The study includes a case example of smartphone-based cardiac anomaly detection, illustrating how portable IoT-enabled devices can support real-time monitoring. This approach reflects the growing trend of integrating mobile health solutions into traditional care frameworks.

Sunny et al. [49] Wearable devices have become a powerful tool in modern healthcare, offering real-time monitoring of physiological parameters such as heart rate, step count, pulse, body fat, and dietary habits. These devices generate large volumes of continuous data, providing an opportunity to improve personal healthcare and early disease detection. Identifying anomalies or outliers in this data—especially in metrics like heart rate—can reveal important health patterns and help detect underlying

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

medical conditions. Due to the sheer volume and complexity of wearable data, manual analysis is impractical, necessitating the use of automated anomaly detection techniques. Recent studies show that over 30% of adults in developed countries now use wearable health devices, with data from these devices becoming increasingly critical in clinical research and decision-making. This article reviews various detection methodologies, including supervised, unsupervised, and semi-supervised learning techniques, each designed to address challenges such as incomplete data and lack of annotations. The paper highlights how machine learning can enhance accuracy in detecting critical health anomalies, ensuring better diagnostics and timely interventions. It also emphasizes the growing use of wearables in clinical studies, demonstrating their expanding role in proactive healthcare. As the global wearable technology market is projected to reach USD 118 billion by 2028, the need for reliable and efficient anomaly detection methods becomes even more vital.

Buiya et al. [50] The Internet of Things (IoT) has become a transformative force, integrating connected devices into nearly all facets of modern life—from smart homes to industrial systems and healthcare infrastructure, particularly in the U.S.A. However, with this widespread adoption comes an urgent need for robust cybersecurity, as IoT systems are increasingly targeted by sophisticated cyberattacks. Traditional rule-based defenses often fall short, prompting the use of machine learning (ML) and artificial intelligence (AI) for detecting and preventing such threats. This research explores the deployment of advanced ML models to identify cyberattacks in IoT network traffic. Using benchmark datasets such as UNSW-NB15, CICIDS2017, and TON_IoT—which include both benign and malicious traffic—the study applied data preprocessing techniques to handle inconsistencies and missing values. Two models were tested: Logistic Regression and Random Forest. While Logistic Regression provided a solid baseline, it underperformed in detecting attacks due to a high false negative rate and lower recall. In contrast, Random Forest showed superior performance across nearly all metrics, with higher accuracy, recall, and precision, making it more reliable for real-world application. This outcome highlights the critical role of ensemble learning models in IoT cybersecurity. With the number of connected IoT devices expected to surpass 29 billion by 2030, enhancing cyber threat detection with ML-driven solutions is more crucial than ever.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

Guo et al. [51] Anomaly detection is a critical aspect of maintaining the reliability and security of IoT systems. This paper addresses a major gap in the field: while many existing approaches focus on cloud-based solutions, they often suffer from high computational costs and limited scalability, especially in edge computing environments. To overcome these challenges, the authors propose an Energy-efficient Graph Neural Network-based Anomaly Detection (EGNN) method designed specifically for multivariate time series data in IoT applications. A notable contribution of this work is its ability to capture inter-device data correlations using a Subgraph Generation Algorithm (SGA). This algorithm identifies subgraph centers, reducing the volume of data needed for regular monitoring. The framework incorporates a mode-switching mechanism that uses a lightweight multi-layer perceptron for standard anomaly forecasting, switching to a more complex graph attention-based model only when potential anomalies are flagged. This dual-mode strategy ensures that energy consumption remains low during normal operations while maintaining high accuracy when anomalies occur. Extensive experiments on real-world datasets validate the system's effectiveness, showing it outperforms current state-of-the-art models in both detection accuracy and energy efficiency. Overall, this work presents a novel and practical approach for edge-level anomaly detection in IoT, making it highly relevant for real-world deployment in resource-constrained environments.

Henandez et al. [52] With the rapid expansion of the Internet of Things (IoT), the attack surface for cyber threats has grown significantly, highlighting the need for robust anomaly-based intrusion detection systems (AIDS). Traditional approaches now incorporate machine learning (ML) and deep learning (DL) techniques to handle vast and complex data flows. However, the success of these models is heavily dependent on the quality of features extracted from the heterogeneous and voluminous IoT traffic. Feature extraction and selection have become bottlenecks due to data diversity, standardization issues, and the sheer scale of generated information. This study presents an innovative ML-based approach that addresses these challenges by integrating locality-sensitive hashing (LSH) as a fingerprinting mechanism. LSH transforms network packet data into a meaningful and compact representation that is suitable for modeling, reducing the reliance on traditional

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

feature engineering. The models used—Decision Trees and Random Forests—are well-suited for interpretability and performance in high-dimensional data environments. The method was evaluated on two widely used benchmark datasets, ToN-IoT and MQTT-IoT, which simulate real-world attack scenarios on IoT networks. The results are highly promising, achieving false positive rate (FPR) of just 0.13%, clearly outperforming existing techniques. This study effectively demonstrates how LSH-based fingerprinting can simplify data preprocessing while maintaining superior detection performance, making it a practical and scalable solution for securing IoT ecosystems.

Saba et al. [53] This study addresses the escalating cybersecurity challenges posed by the widespread adoption of Internet of Things (IoT) technologies, which generate massive data traffic and create new vulnerabilities. With billions of interconnected devices exchanging information in real time, IoT systems have become attractive targets for cyber attackers. Detecting anomalies and cyber intrusions in this complex environment is essential for securing the IoT ecosystem. To tackle this issue, the study employs and compares five machine learning (ML) algorithms—Support Vector Machine (SVM), Artificial Neural Network (ANN), Decision Tree (DT), Logistic Regression (LR), and k-Nearest Neighbours (k-NN)—to evaluate their effectiveness in identifying cyber anomalies within IoT systems. The comparative analysis was conducted using two standard datasets, offering a practical benchmark to assess model performance. The results reveal that Artificial Neural Networks outperformed the other models across key evaluation metrics, particularly the F1 score, achieving a near-perfect score of 0.999. This suggests ANN's superior ability to detect subtle patterns and complex relationships in the data, making it highly suitable for anomaly detection in dynamic IoT environments. Although k-NN, DT, and SVM also performed well, they slightly lagged behind the ANN in precision and recall. Overall, this research provides critical insights into the comparative strengths of various ML approaches for IoT cybersecurity and serves as a reference point for practitioners aiming to implement effective intrusion detection systems in resource-constrained or large-scale IoT deployments.

Liu et al. [54] This study investigates the cybersecurity challenges in edge nodes of power grid IoT systems, which are particularly vulnerable due to their limited security

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

infrastructure. These weak points in the power communication network pose serious risks, as attackers can exploit them to infiltrate critical energy infrastructure, disrupt power distribution, or manipulate sensitive control data. To mitigate these threats, the authors propose a novel anomaly detection method based on attribute graphs, aimed at identifying malicious traffic in power IoT environments. The approach models network traffic as an attribute graph, where each node encapsulates traffic features, and graph neural networks (GNNs) are used to learn from both the topology and attribute data using meta-path-based representation learning. This enables the model to capture complex relational patterns and detect subtle anomalies that traditional methods might miss. To address scalability, particularly with large-scale power IoT datasets, the study introduces a Hoffman encoding-based data adjustment strategy. This technique dynamically optimizes attribute map size and data fidelity, enhancing model performance under varying data conditions. Experimental validation on real-world traffic datasets confirms the effectiveness of the proposed method, showing it can reliably detect anomalies while maintaining high accuracy and efficiency. This research offers a cutting-edge solution to enhance the cyber resilience of smart grid systems, especially at the vulnerable edge node level, making it a valuable contribution to the field of IoT-based power system security.

Caville et al. [55] This paper explores the innovative application of Graph Neural Networks (GNNs) for self-supervised intrusion and anomaly detection in computer networks. Traditional network intrusion detection systems (NIDSs) typically depend on labelled datasets and node-level features, which limit their adaptability to unseen attacks and reduce overall accuracy—especially since they often ignore valuable edge-level (packet-based) information. To overcome these limitations, the authors propose Anomal-E, a GNN-based framework that uniquely leverages edge features and the topological structure of network flows in a self-supervised learning setup. This means the model can learn meaningful representations from raw network traffic without requiring labeled data, significantly improving its generalizability to emerging threats. Unlike prior GNN-NIDS implementations, Anomal-E directly processes network flows as graphs, capturing the relationships between traffic packets more effectively. This is particularly relevant because computer network traffic naturally forms a graph, with nodes representing hosts and edges representing data

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

flow between them. The study evaluates Anomal-E using two widely recognized modern NIDS benchmark datasets, and the results demonstrate superior performance over traditional machine learning baselines and feature-based methods. These findings highlight Anomal-E's promise for real-world, scalable, and robust intrusion detection, especially in complex and evolving network environments. By integrating edge-level learning with self-supervision, Anomal-E sets a new benchmark in anomaly detection research, offering a more adaptive and accurate approach to securing network infrastructures.

Balakrishna et al. [56] The paper explores the increasing complexity of integrating and analyzing massive volumes of IoT sensor data, particularly within the healthcare sector. With approximately 35 billion IoT devices currently connected to the internet and an expected rise to between 80 and 120 billion devices by 2025—generating an estimated 180 trillion gigabytes of new sensor data—the challenge of handling such vast, heterogeneous, and unstructured data becomes critical. Manual integration of this data is no longer feasible due to its scale and diversity in communication protocols and formats. To address this, the authors emphasize the importance of semantic annotation and machine learning techniques as viable solutions for automated data integration and interpretation. The paper proposes a detailed multi-layered framework that includes raw data acquisition, semantic annotation, resource data extraction, semantic reasoning, and clustering. These processes aim to semantically enrich the data and group it effectively for meaningful analysis. The application of clustering techniques, combined with semantic technologies, not only facilitates accurate integration but also accelerates the processing pipeline. The study demonstrates that the proposed framework achieves a data integration accuracy of 92.5%, reduces redundant data interpretation by 38% through semantic reasoning, and improves data processing time by over 40% when compared to traditional methods. These findings highlight the critical role of semantics and machine learning in overcoming the limitations of IoT sensor data management, particularly in healthcare applications.

Ali et al. [57] The paper focuses on enhancing heart disease prediction by developing a smart healthcare system that leverages ensemble deep learning and advanced feature fusion techniques. Given that accurate prediction of heart disease is crucial for early

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

intervention and treatment, the authors aim to overcome the limitations of traditional machine learning systems that struggle with high-dimensional healthcare data. Most existing systems rely on conventional feature selection and generalized feature weighting, which restrict their predictive capabilities. To address this, the proposed framework combines data from IoT sensors and electronic medical records (EMRs) using a feature fusion method that enriches the dataset with meaningful and diverse healthcare information. Irrelevant and redundant features are removed using the information gain technique, thereby reducing computational complexity and improving efficiency. Moreover, feature weights are calculated for each class using a conditional probability approach, adding a level of specificity that improves classification accuracy. An ensemble deep learning model is then trained on the optimized dataset to predict heart disease. The system was rigorously tested against conventional classifiers and demonstrated an impressive accuracy of 98.5%, outperforming existing models. This result establishes the system's superiority in terms of both accuracy and efficiency, proving its value in modern smart healthcare applications for proactive cardiac care.

Bhavasara et al. [58] This study addresses growing security concerns in Internet-of-Things (IoT) networks by proposing an advanced Intrusion Detection System (IDS) based on a deep learning model called Pearson-Correlation Coefficient Convolutional Neural Networks (PCC-CNN). As IoT is increasingly deployed in critical sectors such as transportation, healthcare, agriculture, and military, the vulnerability of these systems to cyber threats due to communication protocol weaknesses has become a major concern. Traditional signature- and rule-based methods have proven inadequate in this context. To overcome this challenge, the authors developed the PCC-CNN model, which first extracts significant linear correlations among features using Pearson-Correlation Coefficient analysis, followed by deep pattern learning through a Convolutional Neural Network. This model supports both binary classification for anomaly detection and multiclass classification for identifying various types of attacks. The performance of the PCC-CNN model was rigorously evaluated using three benchmark datasets: NSL-KDD, CICIDS-2017, and IOTID20. Initially, five machine learning models—Logistic Regression, Linear Discriminant Analysis, k-Nearest Neighbors (KNN), Classification and Regression Tree (CART), and Support

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

Vector Machine (SVM)—were trained using the same PCC-based features. Among these, KNN and CART performed best, achieving accuracies of 98%, 99%, and 98% across the three datasets. However, the PCC-CNN model outperformed all traditional models, achieving a high detection accuracy of 99.89% with a very low misclassification rate of 0.001. For binary and multiclass classification, the false alarm rates were impressively low at 0.02, 0.02, and 0.00, respectively. These results demonstrate that the proposed deep learning-based IDS offers a significantly more robust and accurate solution for securing IoT environments compared to conventional machine learning approaches.

Najim et al. [59] The integration of IoT and wireless sensor networks (WSNs) into healthcare systems has paved the way for smarter patient monitoring solutions, especially with the emergence of high-speed 5G networks. In one recent study, researchers designed an IoT-based health monitoring system powered by artificial neural networks (ANNs) to track vital signs such as blood pressure, heart rate, oxygen saturation, and body temperature. This system aimed to support remote and elderly patients by enabling real-time communication with healthcare providers, even in critical conditions. The ANN model played a key role in feature extraction and analysis, helping achieve a notable accuracy of 96%. The system's performance was validated through comparisons with commercial medical devices, showing minimal relative errors across different health parameters. Additionally, the use of 5G enhanced the system's responsiveness, making it significantly faster than other wireless alternatives. Practical implementation confirmed the model's reliability and efficiency in real-time environments. This framework not only improves monitoring but also facilitates timely medical responses in rural and underserved regions.

Geng Yang et al. [60] In-home healthcare services powered by IoT are gaining attention for their commercial and practical value, yet a complete and scalable platform is still lacking. Addressing this gap, a study introduced the iHome Health-IoT platform, which integrates various smart components to enhance home-based medical care. At the heart of the system is the iMedBox, an open-platform smart medicine box designed for easy device and service integration. Alongside it, the iMedPack uses passive RFID technology and smart materials to track and manage medication, while the Bio-Patch—developed using advanced inkjet printing and

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

system-on-chip technology—serves as a flexible wearable sensor for vital sign monitoring. Together, these components create a seamless healthcare ecosystem that merges wearable sensors, smart packaging, and telemedicine. The platform is user-friendly, efficient, and designed to improve the overall healthcare experience from home. Field trials demonstrated its practicality and confirmed its effectiveness in real-world use, suggesting it could be a significant step toward more accessible and efficient healthcare delivery.

Ali et al. [61] With the global rise in the elderly population, there is a pressing need for smart healthcare systems that can support remote diagnosis in smart homes and cities. To address this, a study proposed an intelligent healthcare system that mimics the human auditory mechanism to detect and classify various vocal fold disorders. The system uses bandpass filters aligned with the Bark scale to replicate how humans perceive sound, enabling it to function like an expert clinician analyzing a patient's voice. The approach focuses on auditory features for high-precision diagnosis of conditions such as vocal fold polyps, keratosis, paralysis, nodules, and adductor spasmodic dysphonia. Experimental results demonstrated exceptional accuracy, reaching 99.72% overall, with individual disorder classification accuracies also exceeding 95%. Notably, when distinguishing paralysis from other conditions, the system achieved 99.13% accuracy. These findings indicate that the system is not only highly accurate but also suitable for practical use in remote vocal health assessments. It outperforms traditional voice disorder diagnosis systems and presents a promising solution for elderly care and telemedicine.

Ke Qi et al. [62] Smart clinical decision support systems are transforming healthcare by enabling early detection of both physical and mental health conditions. In this context, a study proposed a secure and efficient health condition monitoring (HCM) system based on cloud-integrated IoT (C-IoT) architecture. The system uses machine learning algorithms, particularly artificial neural networks (ANN), to analyze large volumes of patient data for accurate and timely diagnosis. Traditional systems often fall short in terms of security and adaptability, which this model addresses by incorporating a lightweight encryption mechanism to protect sensitive clinical data. The system leverages historical patient records stored in the cloud to aid in predictive diagnostics, ensuring personalized and context-aware healthcare. By combining cloud

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

computing with machine learning, the model facilitates proactive intervention and supports doctors in making better-informed decisions. Experimental evaluation demonstrated a diagnostic accuracy of around 91%, showcasing the system's reliability. Overall, this smart C-IoT framework represents a significant advancement in creating secure, intelligent, and scalable solutions for modern healthcare under the vision of Society 5.0.

Sworna et al. [63] The growing integration of IoT and machine learning (ML) has significantly reshaped traditional healthcare practices by enabling smarter, data-driven decision-making. In a recent survey, researchers reviewed the complete pipeline—from IoT sensor data collection to ML deployment—for healthcare applications. The sensing layer gathers data from patients, which is then transmitted and processed using advanced communication and storage technologies. The study introduces a novel taxonomy that outlines key stages in developing IoT-ML healthcare systems, providing a unified view of sensors, network protocols, storage strategies, and ML techniques. It also maps communication protocols used with various IoT devices and delves into the ML pipeline, explaining each step from data acquisition to decision-making. The survey includes a detailed review of existing sensors, development boards, and real-world examples, offering a practical guide for system developers. In addition, it identifies pressing research challenges such as data privacy, ethics, deep learning implementation, and security in wireless body area networks (WBANs). This work serves as a comprehensive reference for researchers, offering both foundational knowledge and future directions in building IoT-ML-powered healthcare systems.

Emre et al. [64] The COVID-19 pandemic has accelerated the adoption of advanced technologies like the Internet of Medical Things (IoMT), Wireless Body Area Networks (WBANs), and cloud computing in healthcare. In response, a study proposed an IoMT framework integrating WBANs with fog and cloud computing to manage and analyze large volumes of health data. In this system, fog computing is used for real-time, lightweight processing, while cloud computing handles more complex and time-consuming analytics. The framework was tested using a diabetes prediction scenario where WBAN-generated data was analyzed using both fuzzy logic and machine learning algorithms. Fuzzy logic was applied at the fog level, achieving a 64% accuracy rate, while support vector machine (SVM), random forest (RF), and

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

artificial neural network (ANN) were applied in the cloud, achieving 89.5%, 88.4%, and 87.2% accuracy respectively. This dual-layer processing model allowed for both quick local insights and deeper cloud-based analysis. The study also evaluated network performance, examining throughput and delay under different node priorities using the IEEE 802.15.6 standard and AODV protocol. Overall, the proposed system showcases an efficient, scalable, and responsive framework for predictive healthcare in pandemic and post-pandemic environments.

Hathaliya et al. [65] The evolution of the healthcare industry from Healthcare 1.0 to 4.0 reflects a major technological shift—from doctor-centric practices to interconnected, intelligent systems powered by IoT, cloud, fog computing, and telehealth. While Healthcare 4.0 improves data sharing and collaboration among stakeholders, it also raises serious concerns about security and privacy. A lack of proper safeguards can lead to data breaches, putting sensitive patient information at risk. Recognizing these challenges, a recent study conducted a detailed review of current methods aimed at securing Healthcare 4.0 environments. The paper explores various frameworks and technologies, particularly highlighting blockchain as a promising solution for ensuring data integrity and privacy. It introduces structured taxonomies to categorize different security issues and provides a comparative analysis of techniques based on their strengths and limitations. The authors also offer insights that are valuable for both researchers and industry professionals, outlining critical areas for future investigation. This work serves as a comprehensive guide for developing secure and privacy-aware systems in the rapidly evolving landscape of digital healthcare.

Mcmurray et al. [66] Software Defect Prediction (SDP) has become increasingly important as software systems grow in complexity and are deeply embedded in everyday life. To enhance the reliability of such systems, a study explored the application of various machine learning (ML) techniques for identifying software defects. The research focused on evaluating and comparing different feature extraction (FE) and feature selection (FS) methods, including Principal Component Analysis (PCA), Partial Least Squares Regression (PLS), Fisher Score, Recursive Feature Elimination (RFE), and Elastic Net. These techniques were tested both independently and in combination with ML algorithms such as SVM, Logistic

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

Regression, Naïve Bayes, KNN, MLP, Decision Tree, and ensemble methods like Bagging, AdaBoost, XGBoost, Random Forest, and Stacking. The study involved an extensive experimental setup to assess how these preprocessing methods influence model performance. Results showed that FE and FS can either enhance or degrade accuracy depending on the method and algorithm used. Notably, PLS stood out for delivering the most consistent performance improvements, while PCA paired with Elastic Net also provided acceptable gains. The findings offer practical guidance for selecting suitable combinations of preprocessing techniques and ML models to improve defect prediction in software development.

Owen et al. [67] In the evolving landscape of IoT networks, securing communication protocols—especially DODAG (Destination-Oriented Directed Acyclic Graph) control messages—is critical, as these are essential for efficient routing in low-power and lossy networks. However, such messages are increasingly targeted by flooding attacks, causing performance degradation. To counter this, a recent project proposed a deep learning-based anomaly detection framework capable of identifying such attacks in real-time. The approach involves collecting a rich dataset comprising both normal and malicious DODAG traffic, followed by preprocessing steps like feature extraction, normalization, and data augmentation to improve learning outcomes. The study evaluates multiple deep learning models, including CNNs, RNNs, and LSTM networks, and considers hybrid architectures to better capture complex traffic patterns. To ensure robustness, the training process integrates dropout, batch normalization, and augmentation techniques. A real-time detection mechanism is also developed to trigger alerts upon spotting anomalies. The system's effectiveness is validated using metrics such as precision, recall, F1-score, and ROC curves, along with comparisons to traditional methods. The study aims to produce a high-performance model that strengthens the detection and prevention of DODAG flooding attacks, offering a scalable and intelligent solution for securing IoT infrastructures.

Zhang et al. [68] In large-scale distributed data stream environments, ensuring real-time data quality and detecting anomalies is a major challenge due to time delays and data degradation. To address this, a study introduced a deep learning-based framework that combines quality-aware feature extraction with adaptive neural networks for real-time monitoring. The system utilizes a multi-dimensional

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

assessment strategy that accounts for temporal and spatial correlations, enabling a more holistic evaluation of data quality. Built on a distributed architecture, it supports parallel processing across multiple nodes, ensuring scalability with minimal latency. A unique aspect of this model is its online learning capability, which allows it to adapt dynamically to changing data patterns and maintain robust performance. The method was tested on three large datasets—industrial IoT (2.5TB), network traffic (1.8TB), and financial transactions (3.2TB)—and showed significant improvement over traditional techniques. It achieved an anomaly detection accuracy of 97.8%, with latency under 10 milliseconds and consistent throughput exceeding 1.2 million events per second. Precision in anomaly detection remained at 95%, and performance scaled linearly up to 128 nodes, making this approach both reliable and efficient for real-time data stream environments.

Zhu et al. [69] High-pressure heaters play a vital role in thermal power plants, and accurate monitoring of their state is crucial for ensuring safety and optimizing operational costs. To address the challenges posed by rapid load changes and prolonged low-load conditions, this study presents an advanced monitoring and state prediction approach. The system leverages historical operational data for effective feature selection and utilizes a hybrid CNN-BiLSTM model to capture both spatial and temporal patterns in the data. Bayesian optimization is applied for fine-tuning hyperparameters, while automated machine learning (AutoML) enhances the model's adaptability to evolving conditions. For anomaly detection and health assessment, an enhanced Support Vector Data Description (SVDD) algorithm is integrated. Tested on real data from a coal-fired power plant, the proposed model achieved low mean squared errors of 1.3260 and 1.4968 for shell-side drain and tube-side outlet temperatures respectively. Its self-learning capability helped reduce MSE by up to 56.98%, and it achieved 96.63% accuracy in detecting anomalies. These results demonstrate the model's reliability and adaptability, making it a strong candidate for real-time, intelligent monitoring of high-pressure heater systems in power generation environments.

Rana et al. [70] This study presents a smart seizure detection system designed for Healthcare IoT applications, addressing the complex challenge of analyzing EEG data to detect epileptic seizures. Epilepsy, characterized by recurring seizures, can result

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

from several causes, including brain injuries, infections, and genetic conditions. Since EEG recordings only capture brain activity during the session, detecting active abnormalities is often uncertain. To overcome the limitations of manual seizure identification, the researchers proposed an automated method that integrates multiple signal processing techniques such as Discrete Wavelet Transform, Hjorth parameters, and statistical features. These features are analyzed using an ensemble of classifiers including Decision Trees, Logistic Regression, and Support Vector Machines, with performance also compared against the kNN classifier and other standard datasets. The system achieved impressive accuracy, reaching up to 100% in some cases, demonstrating the effectiveness of combining diverse classifiers with advanced signal analysis. This real-time approach enhances the potential of IoT in healthcare by supporting timely decision-making for seizure management, thereby improving patient outcomes significantly.

Zahra et al. [71] This study addresses the increasing need for ensuring the safety of elderly individuals living independently, a concern that grows with the aging global population. Leveraging advancements in Ambient Intelligence, the paper proposes a smart home-based solution that offers both cost-effectiveness and improved care. Specifically, the authors introduce a ConvLSTM Autoencoder model tailored to process spatiotemporal data for detecting anomalies in the daily routines and behaviors of elderly residents. Such anomalies are often rare and irregular, making them difficult to identify with conventional methods. The model was validated using two publicly available datasets from the WSU CASAS smart home project and benchmarked against existing state-of-the-art techniques. Experimental results show that the proposed model effectively detects deviations in behavioral patterns, thereby enabling timely interventions. This method holds significant promise in enhancing the safety, autonomy, and overall quality of life for the elderly population through smart home technologies powered by machine learning.

Kishore Kumar et al. [72] This research focuses on addressing the critical need for real-time, accessible, and affordable healthcare solutions, particularly in underserved and remote areas. It introduces a deep learning-based Smart Health Monitoring (SHM) system aimed at non-invasive blood pressure (BP) prediction—an essential aspect of cardiovascular disease management. The proposed solution utilizes a novel ResNet-

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

LSTM neural network architecture, which combines the deep feature extraction capabilities of Residual Networks (ResNet) with the temporal pattern recognition strengths of Long Short-Term Memory (LSTM) networks. The model leverages physiological signals such as ECG and PPG for BP prediction. Through rigorous testing, including Leave-One-Out (LOO) cross-validation and evaluation on an additional dataset, the model demonstrated a mean absolute error (MAE) of 6.2 mmHg and a root mean square error (RMSE) of 8.9 mmHg. While the model incurs a higher computational cost (~4,375 FLOPs), its enhanced accuracy and ability to generalize across different datasets affirm its robustness for continuous BP monitoring applications. The study underscores the feasibility and effectiveness of integrating such AI-driven systems into wearable devices for smart healthcare applications. It also points to the future need for improved anomaly detection mechanisms and real-time cloud-based processing to further enhance remote patient monitoring and clinical decision-making.

Jean et al. [73] With the rapid proliferation of IoT devices, intrusion detection systems (IDS) face increasing challenges in maintaining accuracy, scalability, and computational efficiency, especially when dealing with diverse attack types and data imbalance. Traditional IDS models often fail to offer real-time detection capabilities in large-scale IoT networks, leading to high false positives and missed threats. To overcome these limitations, an Optimized Multiclass Intrusion Classifier (OMIC) was introduced, combining ensemble learning techniques such as LightGBM and XGBoost. The model incorporates dynamic chunk-based processing, adaptive sampling, and cost-sensitive learning to effectively manage class imbalance in vast datasets. Evaluated on the CICIOT2023 dataset comprising over 1 million records and 33 attack classes, OMIC achieved 99.26% accuracy and near-perfect precision, recall, and F1-scores for most DDoS and DoS attacks. This performance significantly surpasses traditional machine learning and deep learning models. However, the study highlights minor shortcomings in detecting web-based and reconnaissance attacks, suggesting future improvements in feature engineering and model sensitivity. Despite this, OMIC demonstrates exceptional performance in real-time IoT environments, offering a scalable and memory-optimized solution for intrusion detection systems in modern smart infrastructure.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

Wli et al. [74] The increasing sophistication of cyber threats, particularly black-box adversarial attacks, poses severe challenges to the reliability of machine learning-based Intrusion Detection Systems (IDS). These attacks exploit model weaknesses by introducing minimal perturbations that result in misclassification, often without requiring access to internal model parameters. Traditional IDSs, which depend on adversarial retraining, struggle to generalize beyond known attack patterns and suffer from high computational costs. To mitigate these limitations, a novel IDS framework has been proposed, incorporating a dual-layered defense mechanism that requires no retraining. Central to this approach is a Credibility Assessment Module (CAM) powered by Explainable AI (XAI) using SHAP values to detect inconsistencies in feature attributions, which signals potential adversarial behavior. Complementing CAM, a secondary defense layer combines Transformer-based semantic payload inspection with behavioral analysis of contextual features, reducing adversarial transferability. Evaluated on realistic datasets such as CSE-CIC IDS 2018 and CIC-IoT 2023, the model demonstrates improved accuracy and resilience under adversarial settings. The proposed architecture surpasses existing adversarially trained IDS frameworks by maintaining high classification integrity and robustness across diverse network environments, thereby setting a new standard for proactive and trustworthy IDS solutions

Cai et al. [75] Network intrusion detection (NID) remains a cornerstone in safeguarding cyberspace, but the inherent data imbalance—where normal traffic vastly outnumbers intrusion traffic—significantly hampers model performance. Existing solutions attempt to reduce majority class samples or oversample minority classes; however, increasing the quantity of intrusion data is more effective for improving model generalizability. This paper introduces a novel intrusion detection framework called DDP-DAR, which integrates feature representation, data augmentation, and detection phases. In the feature representation phase, network traffic is encoded as RGB images by preserving both global and local features. For data augmentation, the model leverages Denoising Diffusion Probabilistic Models (DDPM) enhanced with cosine noise and learnable variance parameters to generate high-quality, balanced RGB traffic images, outperforming traditional generative models like VAE and GAN. Finally, in the detection phase, a dual-attention residual

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

network is employed to extract deep semantic features and enhance the focus on critical intrusion patterns. Experimental results reveal that DDP-DAR surpasses existing augmentation-based NID models across metrics such as Accuracy, F1-score, False Positive Rate, and ROC-AUC, while also demonstrating superior detection stability across multiple scenarios, thereby presenting a robust solution to the data imbalance challenge in modern NID systems.

Gad et al. [76] The exponential growth of Internet of Things (IoT) devices across sectors like transportation and healthcare has increased the demand for secure and efficient operations. However, IoT systems continue to face unresolved challenges related to security, interoperability, and standardization. Addressing these concerns, this study introduces the TOCA-IoT framework—an innovative approach combining explainable artificial intelligence (XAI) and causal inference to improve network anomaly detection. Specifically, the framework employs the Linear Non-Gaussian Acyclic Model (LiNGAM) to uncover causal relationships in IoT network traffic, enabling both high detection accuracy and interpretability. A novel threshold optimization method is also integrated to overcome the challenge of selecting effective anomaly classification thresholds. The framework was evaluated on the CICIoT2023 dataset, a comprehensive IoT attack benchmark. Experimental results demonstrated outstanding performance, achieving a perfect 100% accuracy and 100% F1-score across attack classes. This work underscores the effectiveness of causal discovery methods paired with XAI to build transparent, trustworthy, and accurate anomaly detection systems for IoT networks, especially in high-stakes environments like healthcare and transportation.

Saheed et al. [77] With the proliferation of Cyber-Physical Systems (CPS) integrated within the IoT ecosystem, sectors such as healthcare, energy, and manufacturing now operate in intelligent, interconnected environments. However, this integration introduces critical security and privacy risks, where anomalies or attacks can cause cascading failures. Addressing these concerns, the study presents a novel explainable and privacy-preserving Deep Neural Network (DNN) framework tailored for anomaly detection in CPS-IoT networks. Recognizing the limitations of deep learning models—such as high false positives and limited interpretability—the framework incorporates SHapley Additive exPlanations (SHAP) to provide transparency into the

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

model's decisions. This approach not only assists cybersecurity experts in validating outputs but also improves trust in autonomous systems. Experiments were conducted on two benchmark datasets: Edge-IIoTset and X-IIoTID. The framework achieved 100% accuracy, precision, recall, and F1-score in binary classification tasks, while multi-class classifications attained 99.98% and 99.99% accuracy respectively. In addition to high accuracy, the model exhibited faster training and efficient testing, reinforcing its suitability for real-time intrusion detection in CPS-enabled IoT environments.

Tang et al. [78] As industrial IoT networks grow in complexity, they are increasingly susceptible to sophisticated cyberattacks such as Denial of Service and backdoor intrusions. These attacks often manifest as anomalies in data streams, including traffic spikes, device behavior shifts, or irregular communications. To address the detection of such anomalies amidst dynamic distributions, the authors propose a supervised contrastive learning-based spatiotemporal variational autoencoder (SC-STVAE). This model incorporates a multihead graph attention network (MD-GAT) to capture intricate feature relationships, and a temporal convolution network within the variational autoencoder to learn temporal dependencies. Supervised contrastive learning enhances anomaly detection by improving the distinction between normal and abnormal patterns. To combat data drift, the model uses an event-triggered elastic weight consolidation mechanism that updates weights based on reliability thresholds. Furthermore, a fuzzy entropy-weighted anomaly scoring method improves detection by quantifying reconstruction errors. Evaluation results demonstrate that SC-STVAE outperforms traditional anomaly detection models in terms of accuracy, recall, and F1-score, validating its robustness in dynamic industrial IoT environments.

Qian et al. [79] The Internet of Things (IoT) generates large volumes of multivariate time series data from diverse components such as sensors and controllers, necessitating efficient anomaly detection to prevent system failures or economic loss. Traditional reconstruction-based methods often fall short due to inadequate feature extraction and fusion, coupled with instability in model reconstruction performance. To overcome these challenges, the authors propose RGA_{anomaly}, a novel generative adversarial network (GAN)-based model. It integrates transformers with cross-attention mechanisms to enhance the extraction and fusion of both temporal and

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

metric features from time series data. The architecture comprises a joint generator—combining an autoencoder and a variational autoencoder—and a discriminator to form an adversarial structure. Anomaly scoring is conducted using both reconstruction and discrimination losses, allowing for a more robust and comprehensive anomaly assessment. Experimental results and ablation studies on four publicly available multivariate time series datasets confirm that RGAAnomaly significantly outperforms existing methods in detection accuracy, making it a promising solution for IoT-based anomaly detection applications.

Deivakani et al. [80] Anomaly detection in IoT network traffic plays a crucial role in identifying security threats and abnormal system behavior across complex and heterogeneous networks. To tackle the challenges of accurate and efficient anomaly classification, the authors proposed ADIOT-B3DQRNN-COA—a hybrid framework combining Bidirectional 3D Quasi-Recurrent Neural Networks (Bi-3DQRNN) with the Coati Optimization Algorithm (COA). The approach begins with preprocessing using an Implicit Unscented Particle Filter (IUPF) to eliminate invalid entries from the DS2OS dataset, followed by feature selection through the Archimedes Optimization Algorithm (AOA), which narrows down to seven optimal attributes. These features are classified into eight anomaly types by the Bi-3DQRNN model. To enhance the model's accuracy, COA is employed for optimizing the Bi-3DQRNN parameters. Implemented in MATLAB, the model is rigorously tested using various performance metrics. Results demonstrate that the ADIOT-B3DQRNN-COA method significantly outperforms benchmark approaches like DNN-ADIOT-NTT, DRNN-PSO-IDIIOT, and SMSG-SCADA-SNN, achieving improvements of over 24–32% in accuracy, 19–33% in precision, and marked reductions in error rates, confirming its superiority in anomaly detection across IoT environments.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

2.2 Research Gaps

The rapid integration of IoT devices into the medical industry has significantly enhanced remote monitoring, diagnostics, and patient care. However, the classification of device states remains a critical challenge due to the heterogeneous nature of medical IoT data, which often contains noise, missing values, and inconsistencies. While several machine learning techniques like SVM, KNN, and decision trees have been applied to classify device states, they often fall short in terms of scalability and accuracy when dealing with high-dimensional and real-time data streams. Traditional models are not always effective in handling the dynamic and complex environments found in healthcare IoT systems. Artificial Neural Networks (ANNs) offer a promising alternative due to their ability to learn non-linear patterns and adapt to new data. Nevertheless, existing studies have not sufficiently explored how ANN models can be optimized for specific medical IoT applications, especially under constraints like low-latency requirements and limited computational resources. Most research lacks focus on real-world deployments, often relying on simulated datasets that do not reflect actual hospital or clinical settings. Furthermore, the explainability of ANN-based decisions remains limited, posing challenges for their adoption in critical medical scenarios. The rapid integration of IoT devices into the medical industry has significantly enhanced remote monitoring, diagnostics, and patient care. However, the classification of device states remains a critical challenge due to the heterogeneous nature of medical IoT data, which often contains noise, missing values, and inconsistencies. While several machine learning techniques like SVM, KNN, and decision trees have been applied to classify device states. To bridge these gaps, future research must emphasize the development of lightweight and interpretable ANN architectures tailored for edge-based healthcare applications. Incorporating techniques such as pruning, quantization, and transfer learning can enhance performance on resource-constrained devices. Moreover, integrating ANN models with domain-specific knowledge can improve both accuracy and trustworthiness. Collaborative efforts with healthcare professionals are essential to validate these models in real-time clinical environments. Lastly, building standardized and diverse datasets from real hospital settings can significantly improve model robustness and generalizability.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

2.3 Comparative Study

| S.No | Authors | Title | Existing system | Proposed system | Accuracy | Key findings |
|------|---|---|-----------------------|-----------------|----------|----------------------------------|
| 1 | Akhtar, MD Mobin, Danish Ahamad, Abdallah Saleh Ali Shatat, and Ahmad Saleh Ali Shatat. | Big data classification in IOT healthcare application using optimal deep learning | KNN, fuzzy classifier | DRCO-SRN | 92.9% | Improved classification accuracy |
| 2 | Lee, Jae Dong, Hyo Soung Cha, and Jong Hyuk Park. | M-IDM: A Multi-Classification Based Intrusion Detection Model in Healthcare IoT | Naive bayes , SVM | M-IDM | 98.6% | Higher detection accuracy |
| 3 | Vakili, Meysam, Mohammad Ghamsari, and | Performance analysis and comparison of machine and deep learning | RF, DT ,KNN | RF, DT , KNN | 98% | RF shows high consistency |

**ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF
IOT DEVICE STATES IN MEDICAL INDUSTRY**

| | | | | | | |
|---|--|---|---------|-----------|--------|------------------------------------|
| 4 | Saif, Sohail, Priya Das, Suparna Biswas, Manju Khari, and Vimal Shanmuganathan | HIIDS: Hybrid intelligent intrusion detection system empowered with machine learning and metaheuristic algorithms for application in IoT based healthcare | KNN, DT | GA | 95.39% | GA & DT Gave more accuracy |
| 5 | Als Salman, Dheyaaldin. | A comparative study of anomaly detection techniques for IoT security using adaptive machine learning | SVM | FusionNet | 99% | Gve only High precision and recall |

**ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF
IOT DEVICE STATES IN MEDICAL INDUSTRY**

| | | | | | | |
|---|---|--|-------------|-----------------------------|----------|---------------------------|
| | | for IoT threats | | | | |
| 6 | Khan, Maryam Mahsal, and Mohammed Alkhathami | Anomaly detection in IoT-based healthcare : | RF, DT ,KNN | Advanced processing with SL | 85% | RFDelivers more accuracy |
| 7 | Hasan, Mahmudul, Md Milon Islam, Md Ishrak Islam Zarif, and M. M. A. Hashem | Attack and anomaly detection in IoT sensors in IoT sites using machine learning approach | LR, SVM | DT , RF | 1-2% low | LR , SVM Got less results |

**ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF
IOT DEVICE STATES IN MEDICAL INDUSTRY**

| | | | | | | |
|---|---|---|-----|-------------|-------|-----------------------------|
| 8 | Dwivedi, Rajendra Kumar, Rakesh Kumar, and Rajkumar Buyya.. | Gaussian distribution-based machine learning scheme for anomaly detection in healthcare sensor cloud | SVM | GDA | 98% | High precision |
| 9 | Vishwakarma, Monika, and Nishtha Kesswani | A new two-phase intrusion detection system with Naïve Bayes machine learning for data classification and elliptic | IDS | 2-Phase IDS | 86.9% | Achieved more no hybrid IDS |

**ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF
IOT DEVICE STATES IN MEDICAL INDUSTRY**

| | | | | | | |
|----|--|---|------------------------|-----|-------------------|--------------------------------|
| 10 | Al Abdulwahid, Abdulwahid | "Detection of Middlebox-Based Attacks in Healthcare Internet of Things Using Multiple Machine Learning Models." | XNN | ANN | 98% | Robust and balanced output |
| 11 | Souri, Alireza, Marwan Yassin Ghafour, Aram Mahmood Ahmed | A new machine learning-based healthcare monitoring model for student's condition diagnosis in Internet of Things environment. | Scalable ML Techniques | SVM | 99.0% | SVM gave effective prediction |
| 12 | Tiwari, Anurag, Viney Dhiman, | Patient behavioral analysis with | Rule - Based | ANN | Error margin < 5% | ANN provided accurate reliable |

**ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF
IOT DEVICE STATES IN MEDICAL INDUSTRY**

| | | | | | | |
|----|---|--|--------|---------------|-------|---------------------------------------|
| | Mohamed AM Iesa | smart healthcare and IoT security. | | | | monitoring |
| 13 | Mansour, Romany Fouad, Adnen El Amraoui, Issam Nouaouri | Artificial intelligence and internet of things enabled disease diagnosis model for smart healthcare systems. | LSTM | CSO-CLSTM | 96.5% | Hybrid optimization improved accuracy |
| 14 | Woźniak, Marcin, Michał Wieczorek, and Jakub Siłka. | BiLSTM deep neural network model for imbalanced medical data of IoT systems | BiLSTM | HYBRID BiLSTM | 88% | Combining with DT gave high results |
| 15 | Yousaf, Iqra, Fareeha Anwar, Salma | An Optimized Hyperparameter of | CNN | CNN-HHO | 96% | Increased bug severity findings |

**ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF
IOT DEVICE STATES IN MEDICAL INDUSTRY**

| | | | | | | |
|----|---|---|-------------------------|--------------|-------|--|
| | Imtiaz, Ahmad S. Almadhor , Farruh Ishmanov, | Convoluti onal Neural Network Algorithm for Bug Severity | | | | |
| 16 | Als Salman, Dheyaaldin. | A comparati ve study of anomaly detection technique s for IoT security using adaptive machine learning for IoT threats. | SVM , RF | SVM , RF | 98.5% | Enhanced anomaly detection observed |
| 17 | Shaikh, Naim, M. L. M. Prasad, K. Gowtham i, Vikrant Sharma | Recogniti on of anomaly detection and disturbanc e detection systems in | KNN , NAIVE BAYES | CNN , RNN | 94% | CNN outperfor ms other models |

**ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF
IOT DEVICE STATES IN MEDICAL INDUSTRY**

| | | | | | | |
|----|---|---|------------------------------|-------------------|-------|---|
| | | industrial IOT systems using distributed machine learning | | | | |
| 18 | Sinha, Himanshu . | Analysis of anomaly and novelty detection in time series data using ML | ARIMA , DT - regressor | RF - regressor | 93.7% | RF regressor Delivers more accuracy |
| 19 | Acquah, Gifty, and Hamed Haddadi | Network Anomalies Detection in Smart Grid System using Machine Learning | DT , SVM | HYBRID- IDS | 95% | Reduced more error compared to existing ones. |

**ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF
IOT DEVICE STATES IN MEDICAL INDUSTRY**

| | | | | | | |
|----|--|--|-----------------|---------------------------------------|--------|---|
| 20 | Seba, A.M., Gameda, K.A. & Ramulu. | Prediction and classificat ion of IoT sensor faults using hybrid deep learning model | BiLSTM , MLP | Hybrid model with CNN & LSTM | 96.11% | The hybrid model achieved higher prediction |
| 21 | Ghajari, Ghazal, Ashutosh Ghimire, Elaheh Ghajari,a nd Fathi Amsaad | Network anomaly detection for iot using hyperdim ensional computin g on nsl- kdd. | IDS | HDC | 91% | improving computati onal efficiency and enabling real-time detection with reduced false |

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

CHAPTER 3

EXISTING SYSTEM

3.1 Threshold-Based Monitoring

Threshold-based monitoring involves setting predefined upper and lower bounds for sensor readings or device outputs. If the readings fall outside these thresholds, the system triggers alerts, assuming an anomaly has occurred. This method is simple to implement and is often built into device firmware or hospital monitoring dashboards for vital signs and equipment metrics.

In medical IoT devices, thresholds are typically derived from manufacturer specifications or expert clinical input. For example, a temperature sensor in an infusion pump might trigger a warning if it exceeds 40°C. These limits can work effectively for straightforward parameters, especially when changes beyond certain ranges clearly indicate a malfunction or safety concern.

However, threshold-based systems lack adaptability. Devices may experience gradual wear and tear, which causes performance to drift without necessarily breaching fixed thresholds. Additionally, environmental or patient-specific factors can result in legitimate fluctuations that are falsely flagged as anomalies. The rigid nature of this method makes it unsuitable for dynamic or highly variable operational contexts, which are common in real-world medical environments.

3.2 Scheduled Maintenance and Manual Logging

Scheduled maintenance is one of the oldest forms of manual analysis used to ensure the health and safety of medical equipment. Technicians inspect devices at regular intervals, document operational states, and replace parts or recalibrate as needed. The logbook approach involves keeping detailed written or digital records of observations, service history, and reported anomalies.

In hospital settings, this method is applied across a wide range of devices, from dialysis machines to imaging systems. The analysis is often based on technician experience and historical trends noted during prior maintenance sessions. Some

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

hospitals use checklists to verify device metrics manually, which are then validated by supervisory engineers.

While this method provides a structured overview of device status over time, it suffers from limitations such as subjectivity, human error, and delayed fault recognition. Anomalies that occur between scheduled checks may go unnoticed, and subtle deviations that don't present visible symptoms may be missed entirely. The reliance on manual documentation further introduces inconsistencies and delays in response.

3.3 Visual and Auditory Inspection by Operators

Visual and auditory inspection is a hands-on method where healthcare professionals or technicians detect abnormal device behavior through physical observations. This includes checking for irregular blinking indicators, strange noises, overheating, leaks, or unexpected system reboots. It remains widely used in fast-paced clinical environments where immediate feedback is essential.

Nurses, biomedical engineers, or device handlers are trained to recognize basic visual signs of malfunction or distress. For instance, a beeping alarm on a ventilator or a blinking red LED on a cardiac monitor typically prompts closer examination or device replacement. Such inspections are useful during active patient care or emergencies when rapid judgments are required.

Despite its simplicity, this method is reactive rather than preventive. By the time visible or audible signs appear, the device may already be in a degraded state. Moreover, it requires experienced personnel to identify subtle cues, and fatigue or high workload can reduce attentiveness. It is also not scalable for continuous monitoring across hundreds of devices in a hospital network.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

3.4 Common Problem Statements

- Manual methods lack the ability to detect subtle or emerging faults that develop over time.
- Human error and subjectivity lead to inconsistent analysis and decision-making.
- Periodic checks miss transient faults that occur between inspection intervals.
- These methods are not scalable for large healthcare infrastructures with many IoT devices.
- Manual approaches delay response time, increasing the risk of critical failures during patient care.

CHAPTER 4

PROPOSED SYSTEM

4.1 ANN Feature Extraction

Artificial Neural Networks (ANNs) are utilized in feature extraction tasks to automatically learn high-level abstract representations from input data. Unlike manual feature engineering, ANN-based feature extraction is data-driven and task-specific, allowing the model to learn features that are most relevant to the end objective. This is particularly beneficial in applications such as image classification, anomaly detection, or intrusion detection systems (IDS), where handcrafted features may miss complex relationships. The architecture, training strategy, and activation functions allow ANNs to transform raw input into meaningful features across several hidden layers, making them highly adaptable and scalable for various applications.

Step 1: Input Layer Formation The process begins with feeding the raw data into the input layer of the neural network. This layer is responsible for passing the original input features to the subsequent layers without any modification. Each neuron in this layer represents one feature of the dataset.

Step 2: Hidden Layer Transformation The input data is then passed through one or more hidden layers. Each neuron in these layers computes a weighted sum of its inputs, adds a bias, and applies a non-linear activation function such as ReLU or sigmoid. These transformations help in learning non-linear relationships and abstract patterns in the data.

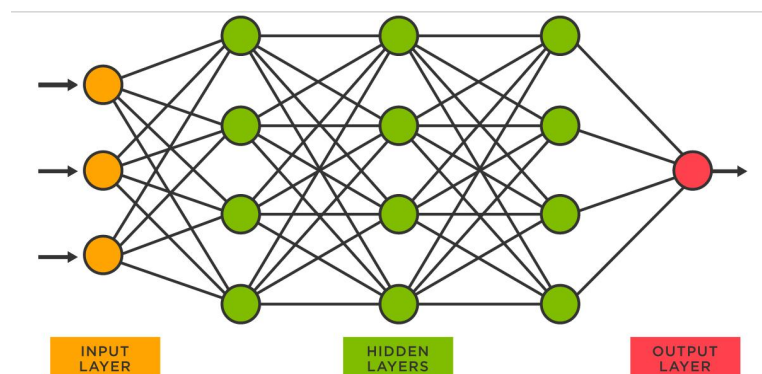


Figure 4.1. ANN Feature Extraction

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

Step 3: Feature Encoding As data propagates deeper through the hidden layers, each layer extracts increasingly abstract and compressed representations of the input data. These intermediate outputs can be considered as learned features. These features are more compact and potentially more informative than the original input, especially in high-dimensional datasets.

Step 4: Feature Vector Extraction At a chosen hidden layer (often the last one before the output), the neuron activations are extracted and treated as the new feature set. These extracted vectors are then used either directly for classification tasks or can be fed into another classifier like SVM, Random Forest, or ensemble methods.

Step 5: Model Training and Optimization The entire network, including the feature extraction layers, is trained using backpropagation to minimize the loss function. The weights are updated iteratively using an optimizer such as Adam or SGD, improving the quality of the learned features over multiple epochs.

4.1.1 Advantages of ANN Feature Extraction

- Automatically learns task-specific features from raw data without manual engineering.
- Capable of capturing complex, non-linear relationships between input variables.
- Provides scalable solutions that can adapt to various data sizes and complexities.
- Offers layered feature abstraction, useful for hierarchical understanding of data.
- Can be fine-tuned or integrated with other classifiers for improved performance.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

4.2 System Architecture

The proposed algorithm integrates a novel hybrid pipeline combining artificial neural network (ANN) based feature extraction with Extra Trees Classification (ETC), built upon Gaussian Naïve Bayes Classification (NBC) pre-filtering. The model begins with Gaussian NBC acting as a probabilistic filter to reduce raw input noise and segment basic data categories from medical IoT devices. The output is passed through an ANN that extracts high-dimensional latent features relevant to device behavior, leveraging multiple hidden layers and ReLU activation for learning non-linear state representations. These extracted features are then classified by an ETC model, which employs ensemble learning to improve classification stability and performance. This three-layered composite design is novel in the IoT medical context, as existing studies rarely employ a sequential combination of Gaussian NBC, ANN feature abstraction, and ETC for binary classification (Normal vs Anomaly).

Step 1: Data Acquisition

IoT device data is collected from medical environments, comprising readings from infusion pumps, ventilators, cardiac monitors, and wearable biosensors. Each record includes timestamped operational states, environmental readings, sensor outputs, and device usage logs. The dataset is labeled manually into two classes: Normal and Anomaly.

Step 2: Preprocessing

The raw data undergoes preprocessing to eliminate redundancy, handle missing values, and normalize ranges. Time-series entries are aligned based on uniform timestamps. Categorical features are encoded using one-hot encoding, and numerical values are scaled using min-max normalization. Outliers are filtered based on interquartile range (IQR) filtering to ensure reliable input for the learning model.

Step 3: Gaussian Naïve Bayes Classification

Before entering the neural network pipeline, the data is filtered using a Gaussian NBC classifier. This probabilistic model assigns prior probabilities to each data point and classifies them into basic

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

normal or anomaly categories. This filtering helps in removing noisy or ambiguous records and reduces computational load for downstream models by narrowing down relevant data segments.

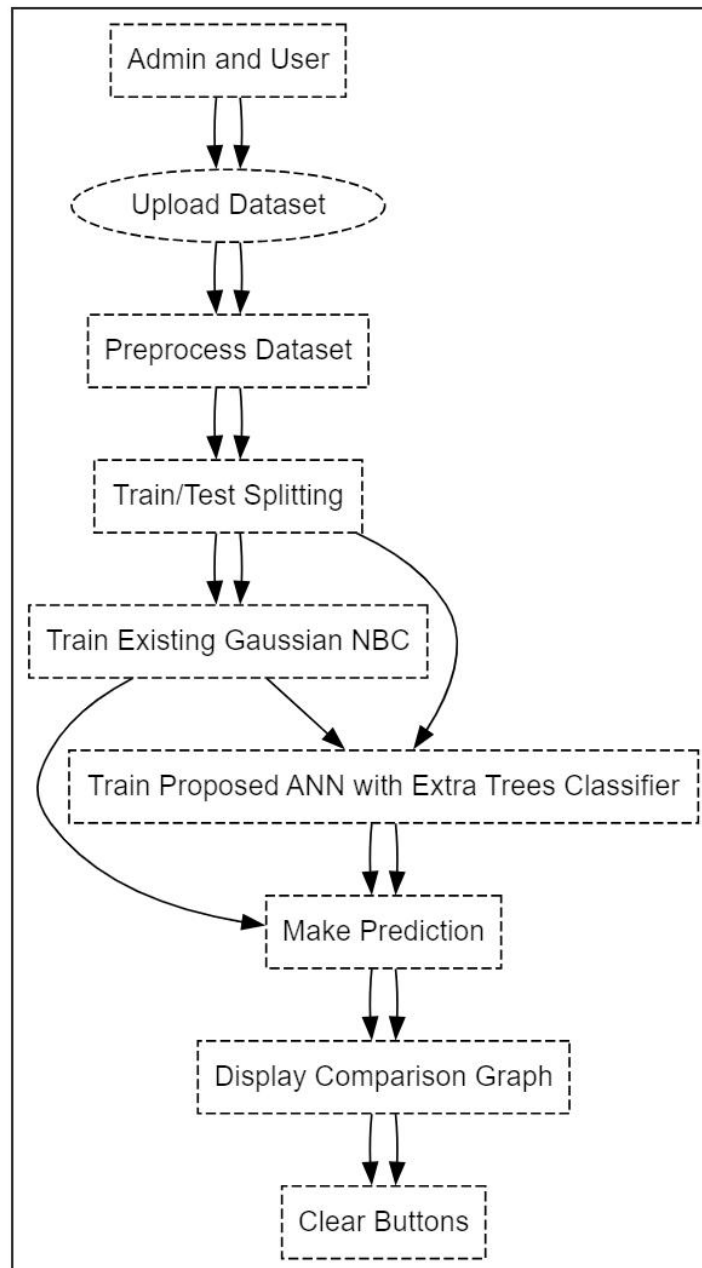


Figure 4.2. Proposed System Architecture.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

Step 4: Feature Extraction using Artificial Neural Network

The NBC-filtered data is then processed by a feedforward ANN model comprising multiple dense layers. Each layer learns abstract, non-linear features from the data using ReLU activation, dropout regularization, and backpropagation-based optimization. The ANN transforms original input space into a latent feature space, highlighting critical device behavior characteristics for classification.

Step 5: Classification using Extra Trees Classifier

The high-level features extracted by ANN are passed into the Extra Trees Classifier. This ensemble model constructs multiple de-correlated decision trees using random feature splits, improving variance reduction and prediction accuracy. The model outputs final binary classifications (Normal or Anomaly) along with feature importance rankings for interpretability.

Step 6: Performance Evaluation

The performance of the hybrid model is evaluated using metrics such as accuracy, F1-score, and confusion matrix analysis. The hybrid model is compared against traditional standalone classifiers to demonstrate its superior detection precision and generalization across diverse IoT device types and patient scenarios.

4.3 Data Preprocessing

The preprocessing method in this application plays a vital role in preparing the dataset for machine learning models, particularly for classification tasks. One of the key advantages is its ability to handle missing data, ensuring that the dataset is clean and ready for further analysis. By dropping missing values, it prevents potential errors or inconsistencies in subsequent steps. Additionally, the method performs label encoding on categorical variables, making them suitable for machine learning algorithms that require numerical input. This transformation ensures that all variables are in a compatible format, optimizing model performance. The visual display of class distribution after encoding also provides insight into the balance of the dataset, which can help assess the need for additional balancing techniques if necessary.

Remove Missing Data: The first step in preprocessing is to clean the dataset by removing rows that contain missing values (NaN). This is achieved using the `dropna()`

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

method, which helps ensure that the data fed into machine learning models is complete and reliable. Missing values can often distort analysis, and by eliminating them, we improve the integrity of the dataset.

Label Encoding for Non-Numeric Columns: In the next step, the method identifies columns that are not numeric (i.e., categorical variables). These columns often contain text or labels that need to be converted into numerical values, as most machine learning algorithms require numerical inputs. The LabelEncoder is used to convert each unique category in the non-numeric columns into a unique integer. This step ensures that categorical data is represented in a form that is interpretable by machine learning models.

Split the Dataset into Features and Target Variables After encoding the categorical columns, the dataset is split into two main components: the feature set (X) and the target variable (y). The target variable, which represents the class labels to be predicted, is isolated from the features, which are the input variables used by the model for prediction. The target variable is stored in the y variable, while the remaining columns are assigned to X.

Class Distribution Visualization To visually analyze the distribution of the target classes after label encoding, a count plot is generated. This count plot displays the frequency of each class in the target variable, providing insights into the balance or imbalance of the dataset. If the classes are imbalanced, it might indicate the need for further steps like oversampling or undersampling to ensure the model performs well across all classes.

Display the Count Plot: The method also annotates the count plot to display the exact number of instances for each class. This provides a more detailed view of the class distribution and helps the user assess whether the dataset requires any further adjustments or preprocessing before moving on to model training.

4.4 Existing GNBC

The Gaussian Naive Bayes Classifier (GNBC) has several drawbacks when applied to real-world problems. One of the main limitations is the assumption of feature independence, which often does not hold true in many practical applications. In cases where features are correlated, this assumption can lead to suboptimal performance.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

Additionally, the GNBC assumes that the features follow a normal distribution (Gaussian distribution). If the data is highly skewed or has outliers, the classifier may not perform well. Furthermore, Gaussian Naive Bayes can struggle with datasets where the features have non-Gaussian distributions or in situations where the class distribution is highly imbalanced. Lastly, despite being computationally efficient, the classifier's performance can degrade significantly when handling complex, high-dimensional data with many irrelevant features.

Input Data: The Gaussian Naive Bayes method begins by receiving the input dataset, which consists of features (independent variables) and the target class (dependent variable). The data is typically split into a training set and a testing set, where the training set is used to learn the parameters of the model, and the testing set is used to evaluate its performance.

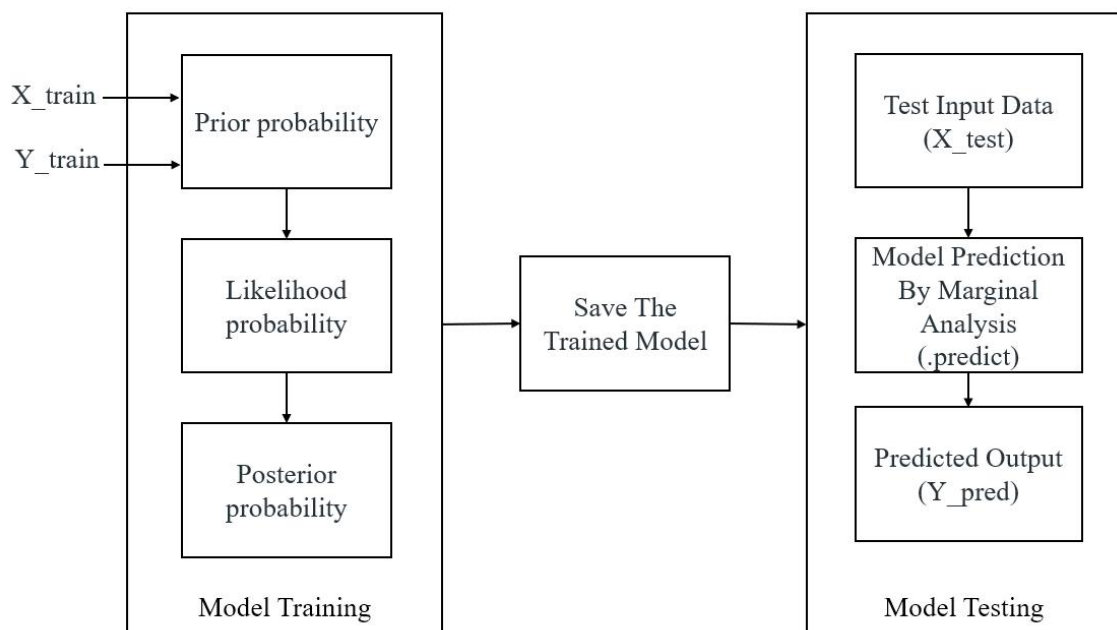


Figure 4.4. Existing GNBC Block Daigram.

Feature Distribution Assumption: The next step in the method is to assume that the features are conditionally independent given the target class. This assumption simplifies the model and makes the computation more efficient. For each feature, the method assumes a Gaussian (normal) distribution, where the feature values are distributed in a bell curve. This assumption enables the model to estimate the mean and standard deviation for each feature for every class label.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

Parameter Estimation: In this step, the Gaussian Naive Bayes classifier estimates the parameters of the Gaussian distribution for each feature and each class label. Specifically, it calculates the mean and standard deviation of the feature values for each class in the training set. These parameters are crucial for calculating the likelihood of a given feature value under each class.

Class Probability Calculation: For each instance in the dataset, the method calculates the probability of the instance belonging to each class. This is done using Bayes' Theorem, which combines the prior probability of each class with the likelihood of observing the given feature values under that class's Gaussian distribution. The classifier assumes that the likelihood of each feature is independent, so the overall likelihood is the product of the individual feature likelihoods.

Prediction: The final step is to assign the class label to each instance. This is done by selecting the class with the highest posterior probability, which is the class that maximizes the product of the prior probability and the likelihood of the observed features. The class with the highest calculated probability is then predicted as the output for the instance.

Output Predicted Labels: The classifier outputs the predicted class labels for the test data based on the calculated probabilities. These predicted labels are then compared to the true labels in the test set to evaluate the performance of the classifier, typically using metrics like accuracy, precision, recall, and F1-score.

4.4.1 Drawbacks

- **Assumption of Feature Independence:** GNBC assumes that all input features are conditionally independent given the class label, which rarely holds true in real-world data. When features are correlated, the classifier's predictions can become inaccurate.
- **Assumes Gaussian Distribution:** GNBC specifically models features using a normal (Gaussian) distribution. This is a limitation for datasets where feature distributions are non-Gaussian, skewed, or have heavy tails, resulting in poor estimation of likelihoods.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

- **Sensitive to Irrelevant Features:** The model can be negatively impacted by noisy or irrelevant features. Since all features contribute multiplicatively to the final probability, even unimportant features can skew predictions.
- **Poor Performance with Imbalanced Data:** GNBC tends to be biased towards the majority class in imbalanced datasets because it does not incorporate any mechanism to handle class imbalance directly, which can reduce its effectiveness in such cases.
- **Limited in Handling Complex Decision Boundaries:** GNBC constructs linear decision boundaries and thus struggles with datasets requiring non-linear separation. It is often outperformed by more complex models like decision trees or ensemble methods when the decision surface is not linearly separable.

4.5 ETC Classifier

The Extra Trees Classifier (ETC), also known as Extremely Randomized Trees, is an ensemble learning method that aggregates the results of multiple unpruned decision trees to improve classification accuracy. Unlike traditional decision tree models, ETC introduces randomness both in the selection of data samples and in the choice of split points, which enhances model diversity and robustness. This makes it particularly useful in applications where overfitting needs to be minimized while maintaining high predictive performance. It is highly effective for high-dimensional datasets and classification tasks where feature relationships are complex and nonlinear.

Step 1: Data Sampling The ETC begins by generating multiple trees using the entire dataset or random subsets of the training data. Unlike Random Forest, it does not always rely on bootstrapped samples, which can reduce variance and increase speed.

Step 2: Random Feature Selection For each split in the decision trees, a random subset of features is selected. This randomization encourages de-correlation among trees and enhances the ensemble's generalization capability.

Step 3: Random Threshold Splitting Instead of calculating the best threshold to split the data, ETC randomly selects thresholds for each candidate feature. This adds an

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

additional layer of randomness, making the trees more diverse and less prone to overfitting.

Step 4: Tree Construction Each decision tree in the ensemble is grown to its maximum depth without pruning. The high depth allows the model to capture intricate data structures, while the ensemble mechanism helps avoid overfitting.

Step 5: Voting Mechanism for Prediction Once all trees are built, a majority voting strategy is used for classification. Each tree contributes one vote, and the class receiving the most votes is selected as the final prediction. This ensemble decision improves reliability and accuracy.

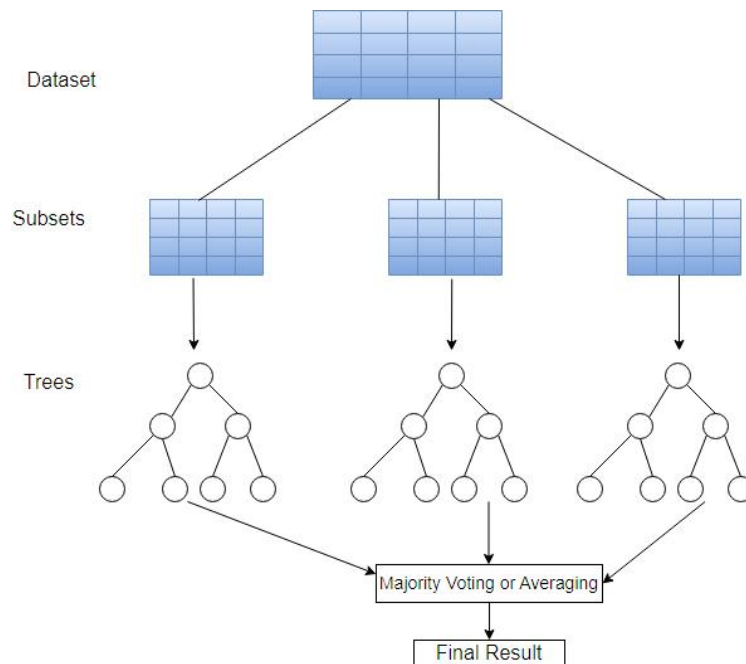


Figure 4.5. ETC Classification.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

CHAPTER 5

UML DIAGRAMS

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group. The goal is for UML to become a common language for creating models of object-oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML. The Unified Modeling Language Is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non-software systems. The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems. The UML is a very important part of developing objects-oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

The primary goal of Unified Modeling Language (UML) is to provide a standardized way to visualize the design of a software system, ensuring consistency and clarity across development teams. It aims to bridge the communication gap between stakeholders by offering a common modeling language for both technical and non-technical participants. UML facilitates the specification, construction, and documentation of software system components, enhancing understanding and collaboration. It supports the development of object-oriented systems by offering a set of best practices and graphical tools to represent system architecture. By using UML, teams can model both software and non-software systems, including business processes. Another important goal is to promote reusability and scalability in system design. Overall, UML serves as a foundational tool for managing complexity in modern software engineering.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

1. Class Diagram

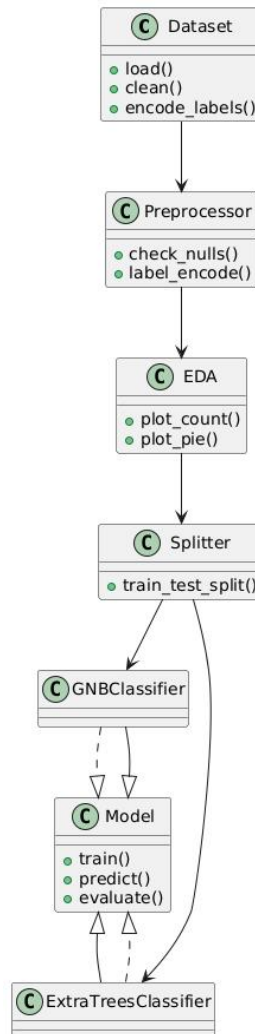


Fig. 5.1: Class Diagram.

This class diagram represents the main components of the project. The Dataset class handles data loading and cleaning. Preprocessor manages null checks and label encoding. EDA creates visualizations. Splitter divides data into training and testing sets. Two classifier classes inherit from the base Model class, representing the GNB and Extra Trees classifiers, which handle training, prediction, and evaluation.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

2. Activity Diagram

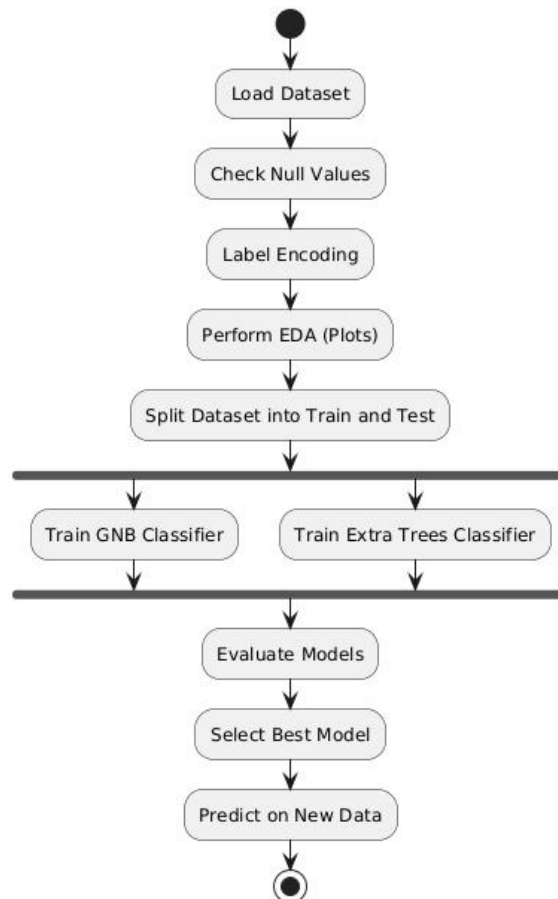


Fig. 5.2: Activity Diagram.

This activity diagram details the step-by-step workflow of the project, from dataset loading to final prediction. It shows the parallel training of GNB and Extra Trees classifiers after preprocessing and EDA, followed by evaluation and selection of the best model for prediction.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

3. Use Case Diagram

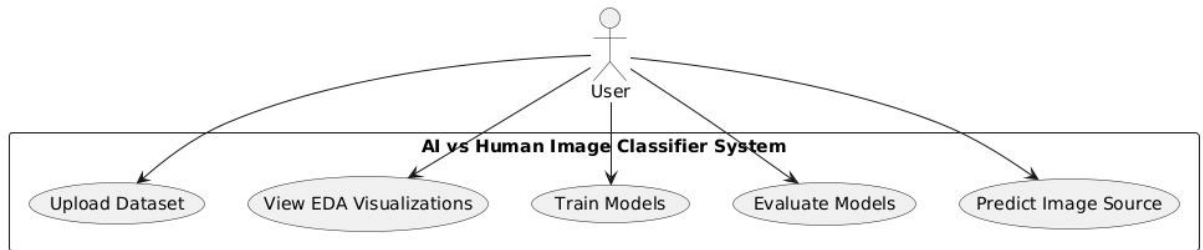


Fig. 5.3: Use case Diagram.

This use case diagram outlines the interactions between the user and the system. The user uploads the dataset, views exploratory visualizations, trains and evaluates models, and uses the system to predict whether an image is AI-generated or human-generated.

4. Sequence Diagram

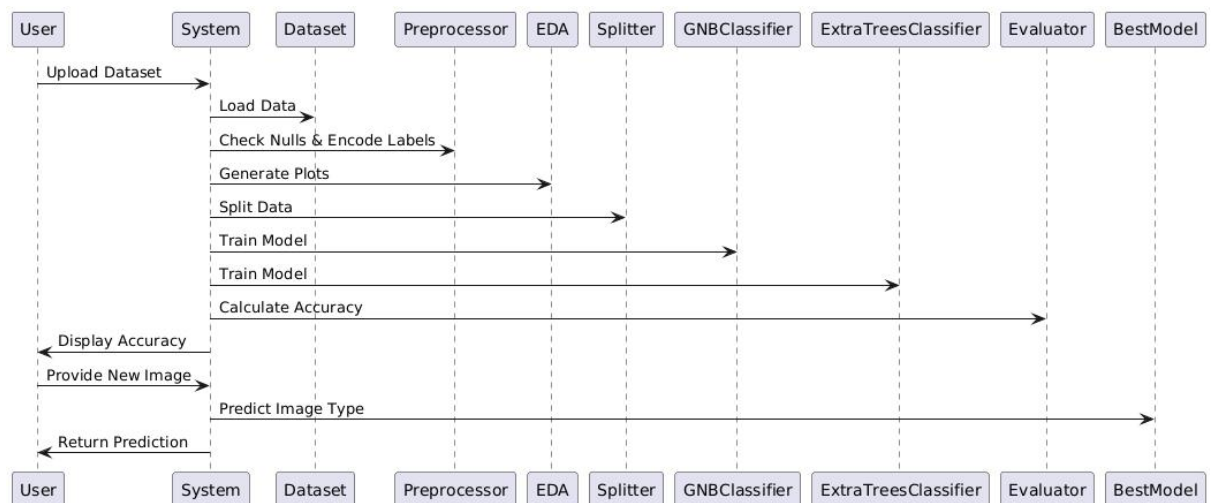


Fig. 5.4: Sequence Diagram.

The sequence diagram captures the chronological flow between the user and system modules. After dataset upload, preprocessing and EDA run sequentially, followed by training classifiers and evaluation. The system finally predicts new image types based on the trained best model.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

5. Dataflow Diagram

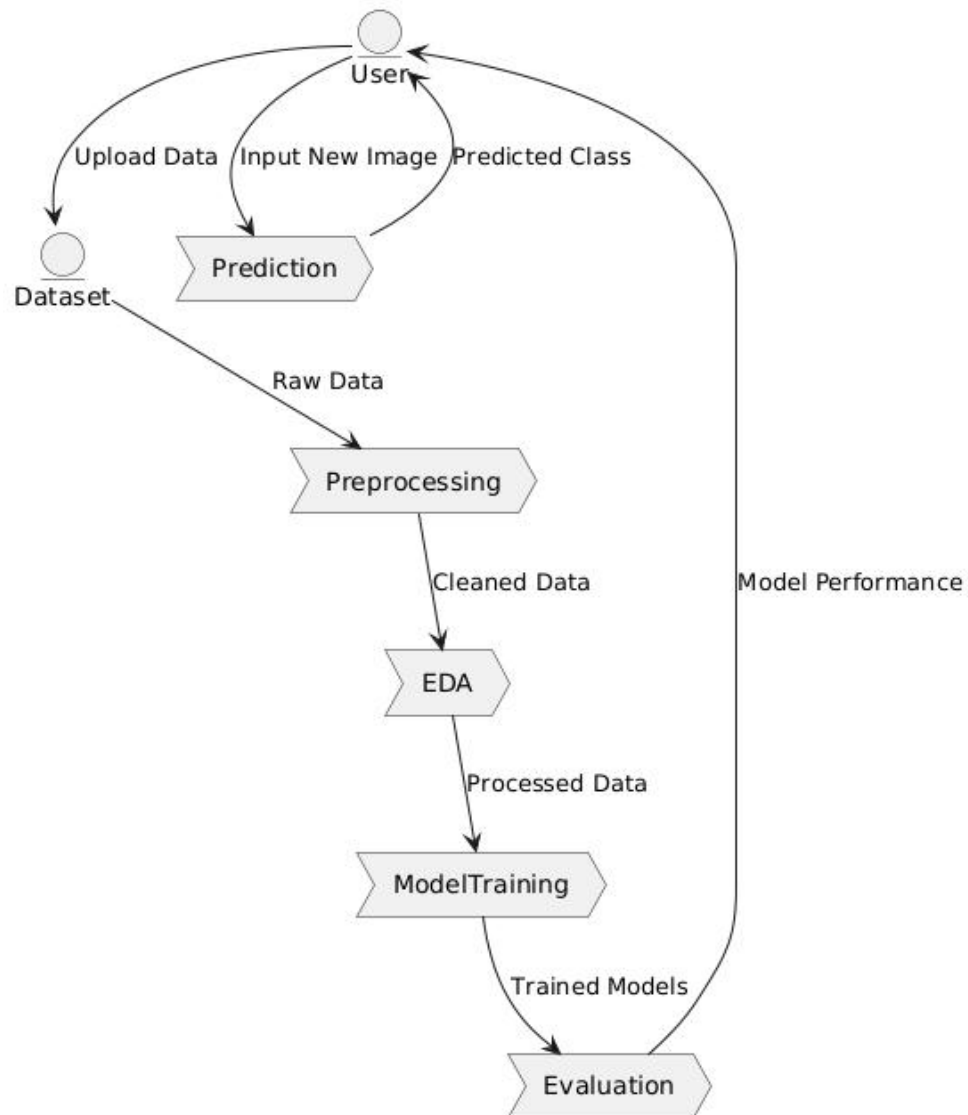


Fig. 5.5: Dataflow Diagram.

The data flow diagram illustrates how data moves through the system. User uploads raw data, which is pre-processed and visualized. Models are trained and evaluated, and finally predictions are delivered back to the user based on new input.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

6. Deployment Diagram

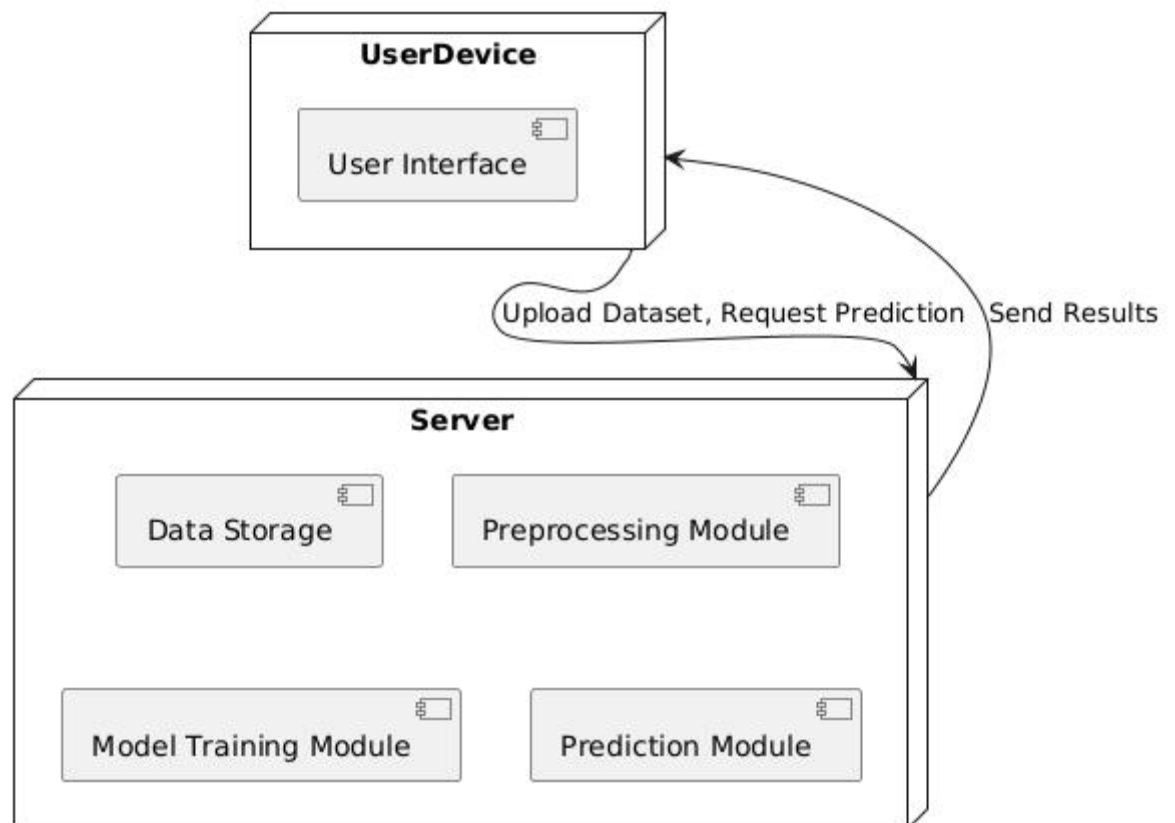


Fig. 5.6: Deployment Diagram.

This deployment diagram represents the physical architecture. The user interacts via a device running the user interface. The server hosts data storage, preprocessing, model training, and prediction modules, processing the user's requests and returning results.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

7. Architectural Block Diagram

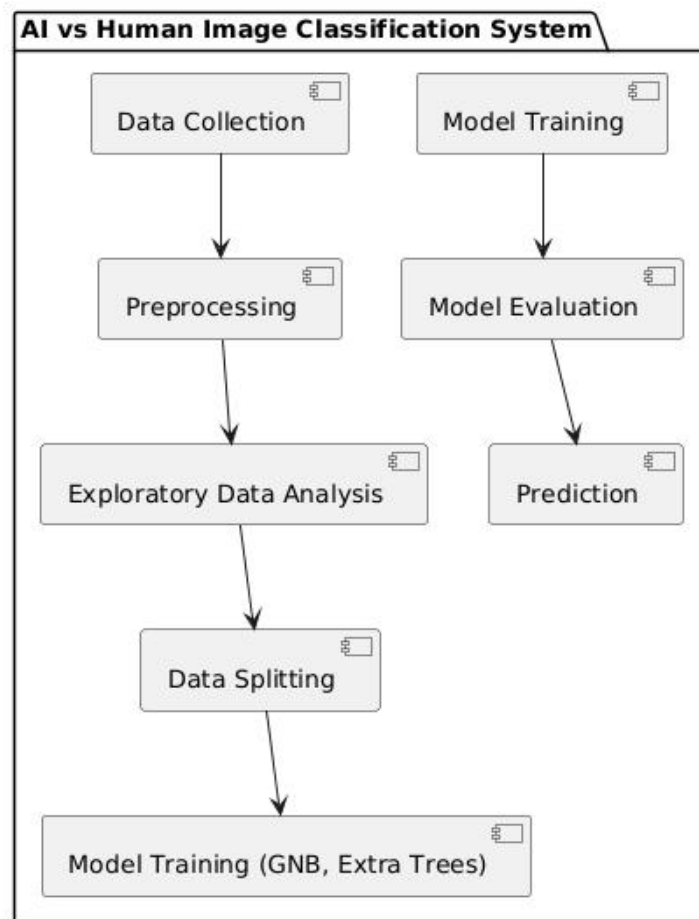


Fig. 5.7: Architectural Diagram.

The architectural block diagram depicts the high-level flow of the project. It starts with data collection, moves through preprocessing and EDA, then data splitting. Next is model training using two classifiers, followed by evaluation and the final prediction phase, illustrating the entire pipeline clearly.

CHAPTER 6

SYSTEM ENVIRONMENT

6.1 Software Requirements

Python 3.7.6 serves as a pivotal version for developers and researchers due to its robust features, backward compatibility, and widespread support across a variety of libraries and frameworks. Released during a time when machine learning and data science tools were rapidly evolving, Python 3.7.6 provided a stable and consistent platform. This version includes critical improvements like enhanced asyncio functionality for asynchronous programming, increased precision for floating-point numbers, and optimized data structures. It became the go-to version for compatibility with popular libraries like TensorFlow 2.0, PyTorch, and Pandas, ensuring seamless integration and efficient execution for both academic and industrial applications.

Compared to older Python versions, 3.7.6 introduced several features such as dataclasses, which simplified boilerplate code for object-oriented programming. The improved async and await syntax made concurrent programming more intuitive, while changes to the standard library enhanced usability and performance. Over newer versions, Python 3.7.6 remains a preferred choice for legacy systems and researchs requiring compatibility with libraries that may not yet support the latest Python updates. Its combination of stability and maturity ensures that it is reliable for long-term researchs, especially in environments where upgrading the Python interpreter might disrupt existing workflows.

6.1.1 TensorFlow Environment

TensorFlow provides a comprehensive ecosystem for building, training, and deploying machine learning models. Its support for numerical computation and deep learning applications makes it a staple in AI research and development. By offering a flexible architecture, TensorFlow enables deployment across a variety of platforms, including desktops, mobile devices, and the cloud. The ability to scale across CPUs, GPUs, and TPUs ensures that TensorFlow is suitable for both small experiments and large-scale production systems.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

TensorFlow's transition from older versions, like 1.x, to 2.x brought significant improvements in ease of use, including the introduction of the `tf.keras` API for building models, eager execution for dynamic computation, and enhanced debugging capabilities. Compared to newer frameworks, TensorFlow retains a strong advantage due to its mature community support, extensive documentation, and integration with TensorFlow Extended (TFX) for managing production pipelines. Its compatibility with other libraries and tools, such as Keras and TensorBoard, makes it a robust choice for end-to-end machine learning solutions.

6.1.2 Packages Overview

NumPy: Version 1.19.5 introduced critical bug fixes and performance enhancements over older versions, especially for operations involving large datasets. The improved random number generator and better handling of exceptions provide more reliable results for numerical computations. This version remains compatible with a wide range of dependent packages. While newer versions optimize speed further, 1.19.5 balances stability and compatibility, ensuring fewer compatibility issues with older software stacks.

Pandas: Version 0.25.3 brought significant speed improvements for large-scale data processing, particularly in operations like `groupby`. Enhancements in handling missing data and improved compatibility with external libraries made this version more robust for data analysis tasks. While newer versions do not add features like enhanced type checking, 0.25.3 remains lightweight and stable for researches that do not require cutting-edge functionalities, making it a practical choice for legacy systems.

Scikit-learn: Version 0.23.1 included improved support for cross-validation and hyperparameter optimization. Updates to `RandomForestClassifier` and `GradientBoostingClassifier` increased model accuracy and efficiency. 0.23.1 is widely tested and compatible with older hardware, making it a dependable choice for environments where the latest versions may introduce compatibility issues.

Matplotlib: Version 3.x improved plot interactivity and introduced better 3D plotting capabilities. The `tight_layout` function and compatibility with modern libraries streamlined visualization workflows. The earlier versions maintain stability and

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

compatibility with older datasets and software, avoiding potential issues from newer, untested updates.

Seaborn: Improved APIs in newer versions simplified aesthetic customization of plots. The addition of new themes and color palettes in 0.11.x enhanced visual appeal for exploratory data analysis. Older versions remain computationally less demanding, suitable for lightweight applications without requiring extensive customizations.

Joblib: A Python library designed for efficient serialization and deserialization of large data, especially useful with NumPy arrays. It is commonly used in machine learning projects to save and load trained models in .pkl format. Compared to the traditional pickle module, joblib offers better performance for large numerical data, making it ideal for heavy computational tasks. With `joblib.dump()`, models can be saved to disk, and `joblib.load()` is used to retrieve them later without the need to retrain. This makes it a valuable tool in developing scalable and reusable machine learning pipelines.

Tkinter: the standard graphical user interface (GUI) toolkit included with Python, used to create desktop applications. It provides a variety of widgets like buttons, labels, text fields, and menus that help developers build interactive interfaces easily. Being cross-platform and lightweight, it is especially popular among beginners for creating quick GUI prototypes.

Label Encoding Tools: Part of Scikit-learn or Pandas utilities were utilized for converting categorical variables into numerical format, essential for model compatibility.

Jupyter: Jupyter improved the interactivity and scalability of notebooks for collaborative coding and visualization tasks. Integration with tools like Matplotlib made it a preferred environment for data exploration. Earlier versions are stable and lightweight, avoiding potential issues with dependencies introduced in newer releases.

6.1.3 Python Installation Procedure

Step 1: Download Python 3.7.6 Visit the official Python website by clicking the following link: <https://www.python.org/downloads/release/python-376/>. Scroll down the page until you reach the "Files" section. Locate the downloadable file for your

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

operating system (e.g., Windows, macOS, or Linux) and click the corresponding link to start the download.

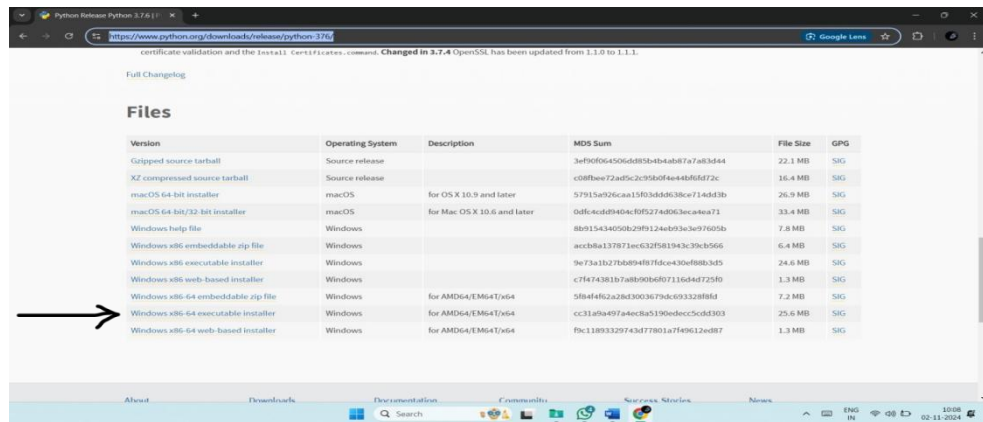


Fig 6.1.1 Locating the downloadable file

Step 2: Verify the Downloaded File: Once the download is complete, you will have the Python 3.7.6 installer file on your system. Ensure the file matches your operating system (e.g., a .exe file for Windows or a .pkg file for macOS) before proceeding to the next step. Click “Add Python 3.7 to Path”, which creates the environmental variables in OS. So, the user will get access to the python with command prompt.

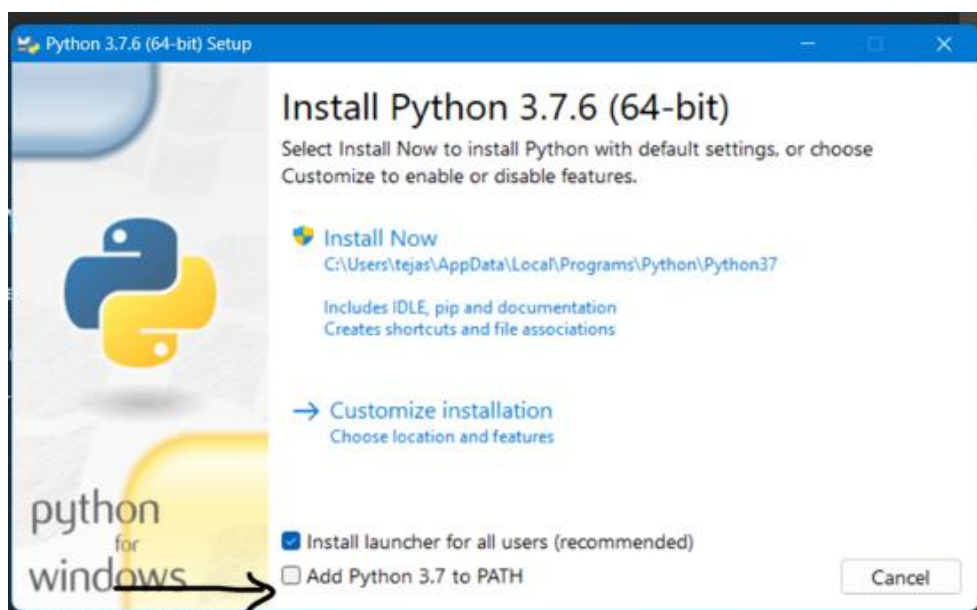


Fig 6.1.2 Installation Setup on Windows – Select Installation Options

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

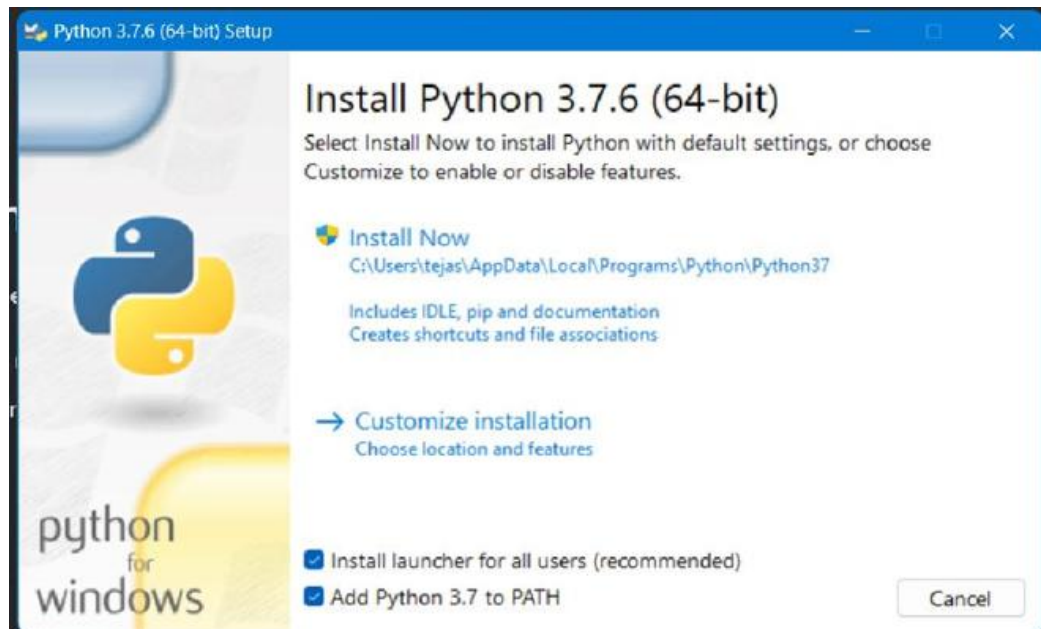


Fig 6.1.3 Selection Process

Step 3: Begin the Installation Process: Open the downloaded Python installer file. During the installation setup, you will see an option labeled "Add Python 3.7 to PATH." Make sure to check this box to ensure Python is added to your system's environment variables, allowing you to run Python from the command line easily.

Step 4: Install Python: After checking the "Add Python 3.7 to PATH" box, click the "Install Now" button to start the installation. Wait for the installation process to complete. Once finished, you will see a confirmation message indicating that Python 3.7.6 has been successfully installed.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY



Fig 6.1.4 Installing Python 3.7.6: Add to PATH and Click Install Now

Step 5: Verify the Installation: Open the Command Prompt (on Windows) or Terminal (on macOS/Linux). Type "python --version" and press Enter. If the installation was successful, the output should display "Python 3.7.6." This confirms that Python is correctly installed and accessible.

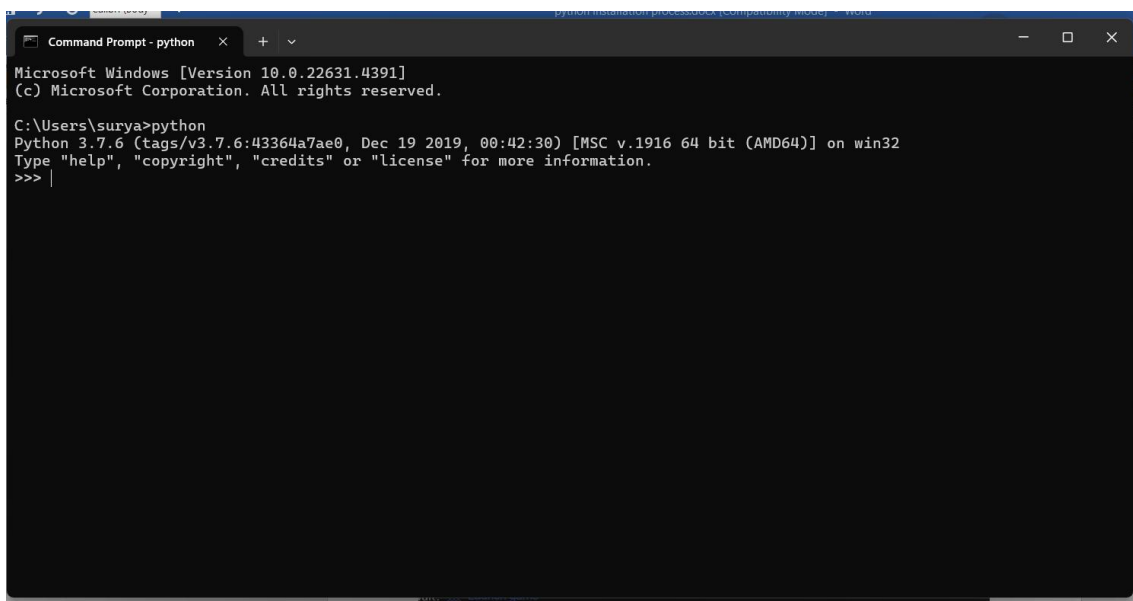
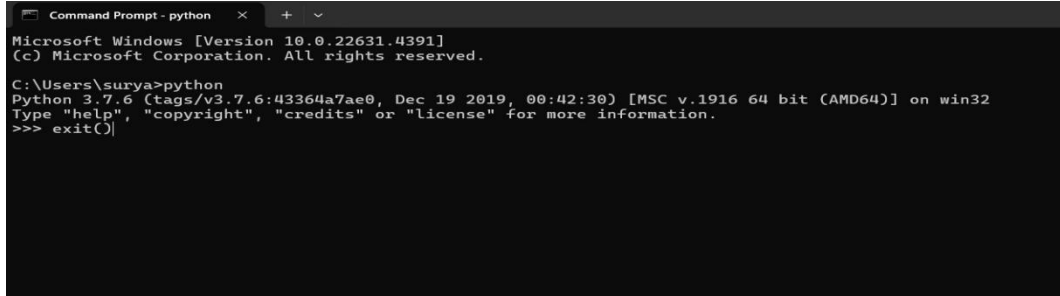


Fig 6.1.5 Command prompt

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

Step 6: Exit the Python Interpreter: If you entered the Python interactive shell by typing "python," exit it by typing "exit()" and pressing Enter. This will return you to the Command Prompt or Terminal.



```
Command Prompt - python
Microsoft Windows [Version 10.0.22631.4391]
(c) Microsoft Corporation. All rights reserved.

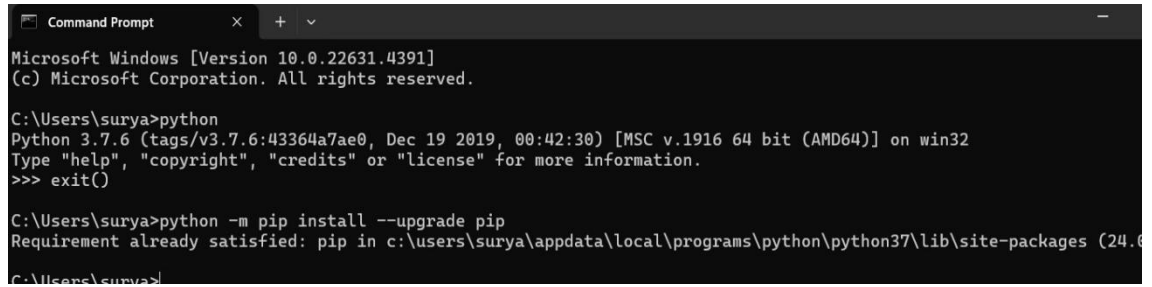
C:\Users\surya>python
Python 3.7.6 (tags/v3.7.6:43364a7ae0, Dec 19 2019, 00:42:30) [MSC v.1916 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> exit()
C:\Users\surya>
```

Fig 6.1.6 Verifying python installation

Step 7: Install the Required Packages: Use the following commands to install the necessary Python packages. Enter each command one by one in the Command Prompt or Terminal, pressing Enter after each. These commands will upgrade pip (Python's package manager) and install the specified versions of the required libraries:

- `python -m pip install --upgrade pip`
- `pip install tensorflow==1.14.0`
- `pip install pandas==1.3.5`
- `pip install scikit-learn==1.0.2`
- `pip install matplotlib==3.2.2`
- `pip install seaborn==0.12.2`
- `pip install numpy==1.19.2`
- `pip install jupyter`

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY



```
Command Prompt
Microsoft Windows [Version 10.0.22631.4391]
(c) Microsoft Corporation. All rights reserved.

C:\Users\surya>python
Python 3.7.6 (tags/v3.7.6:43364a7ae0, Dec 19 2019, 00:42:30) [MSC v.1916 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> exit()

C:\Users\surya>python -m pip install --upgrade pip
Requirement already satisfied: pip in c:\users\surya\appdata\local\programs\python\python37\lib\site-packages (24.0)
C:\Users\surya>
```

Fig 6.1.7 Showcasing python version

6.2 Hardware Requirements

Python 3.7.6 can run efficiently on most modern systems with minimal hardware requirements. However, meeting the recommended specifications ensures better performance, especially for developers handling large-scale applications or computationally intensive tasks. By ensuring compatibility with hardware and operating system, can leverage the full potential of Python 3.7.6.

Processor (CPU) Requirements: Python 3.7.6 is a lightweight programming language that can run on various processors, making it highly versatile. However, for optimal performance, the following processor specifications are recommended:

- **Minimum Requirement:** 1 GHz single-core processor.
- **Recommended:** Dual-core or quad-core processors with a clock speed of 2 GHz or higher. Using a multi-core processor allows Python applications, particularly those involving multithreading or multiprocessing, to execute more efficiently.

Memory (RAM) Requirements: Python 3.7.6 does not demand excessive memory but requires adequate RAM for smooth performance, particularly for running resource-intensive applications such as data processing, machine learning, or web development.

- **Minimum Requirement:** 512 MB of RAM.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

- **Recommended:** 4 GB or higher for general usage. For data-intensive operations, 8 GB or more is advisable.

Insufficient RAM can cause delays or crashes when handling large datasets or executing computationally heavy programs.

Storage Requirements: Python 3.7.6 itself does not occupy significant disk space, but additional storage required for Python libraries, modules, and researchs.

- **Minimum Requirement:** 200 MB of free disk space for installation.
- **Recommended:** At least 1 GB of free disk space to accommodate libraries and dependencies.

Developers using Python for large-scale researchs or data science should allocate more storage to manage virtual environments, datasets, and frameworks like TensorFlow or PyTorch.

Compatibility with Operating Systems: Python 3.7.6 is compatible with most operating systems but requires hardware that supports the respective OS. Below are general requirements for supported operating systems:

- **Windows:** 32-bit and 64-bit systems, Windows 7 or later.
- **macOS:** macOS 10.9 or later.
- **Linux:** Supports a wide range of distributions, including Ubuntu, CentOS, and Fedora.

The hardware specifications for the OS directly impact Python's performance, particularly for modern software development.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

CHAPTER 7

FUNCTIONAL REQUIREMENTS

Functional requirements are detailed statements that specify what a system should do. They describe the system's behavior, functions, and services, outlining how it responds to certain inputs, performs tasks, and interacts with users or other systems. Essentially, they answer the question, "What should the system do?" Here are some key aspects:

- **Functionality:** They define the specific functions or operations that the system must perform.
- **Inputs and Outputs:** They detail the types of inputs the system accepts and the outputs it produces.
- **User Interactions:** They describe how users interact with the system, including command inputs, error handling, and responses.
- **Data Management:** They outline requirements related to data storage, retrieval, and processing.
- **System Behavior:** They specify how the system behaves in various scenarios, including normal operations and exceptional conditions.

Below is a breakdown of the functions used in the research along with their requirements. These “function requirements” describe what each function is responsible for, the expected inputs, processing steps, and outputs or side effects. This can serve as a high-level specification for each function in the research.

1. Requirement Analysis Phase

The requirement analysis phase focuses on identifying the core functionalities needed for the IoMT (Internet of Medical Things) classification application. This phase defines the system's purpose, user roles (Admin and User), and the primary tasks the application must perform to process and classify IoT device states in the medical industry.

FR1: User Role Differentiation

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

- The system shall provide two distinct user roles: Admin and User, each with specific functionalities.
- Admin users shall have access to dataset uploading, preprocessing, train-test splitting, and classifier training.
- User users shall have access to prediction and performance comparison functionalities.

FR1.2: Dataset Management

- The system shall allow Admin users to upload CSV datasets containing IoT device state data.
- The system shall display the loaded dataset's file path and a preview of its contents.

FR1.3: Data Preprocessing

- The system shall preprocess datasets by handling missing values and encoding non-numeric columns using LabelEncoder.
- The system shall display a count plot of the target variable ("attack") after preprocessing.

FR1.4: Machine Learning Model Training

- The system shall allow Admin users to split the dataset into training and testing sets.
- The system shall support training of an existing Gaussian Naive Bayes Classifier (NBC) and a proposed MLP with Extra Trees Classifier.
- Trained models shall be saved for reuse to avoid retraining.

FR1.5: Model Evaluation and Prediction

- The system shall calculate and display performance metrics (accuracy, precision, recall, F1-score, sensitivity, specificity) for trained models.
- The system shall generate and display confusion matrices for model evaluation.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

- The system shall allow User users to upload a dataset for prediction and display predicted outcomes for each row.

FR1.6: Performance Comparison

- The system shall provide a comparison graph to visualize performance metrics of the existing and proposed classifier

2. System Design Phase

The system design phase translates the requirements into a detailed blueprint, specifying the user interface, data flow, and processing logic. This phase ensures that the application's architecture supports all functional requirements efficiently.

FR2.1: User Interface Design

- The system shall provide a Tkinter-based GUI with a full-screen window, a title label, and a text area for displaying logs and results.
- The system shall include persistent "ADMIN" and "USER" buttons to toggle between role-specific functionalities.
- Admin-specific buttons shall include "IoMT Dataset," "Preprocess Dataset," "Train Test Splitting," "Existing Gaussian NBC," and "Proposed ANN with Extra Trees Classifier.
- User-specific buttons shall include "Prediction" and "Comparison Graph."

FR2.2: Dataset Processing Workflow

- The system shall use filedialog to allow dataset uploads in CSV format.
- The system shall use pandas to read and process datasets, ensuring compatibility with machine learning models.
- Non-numeric columns shall be encoded using scikit-learn's LabelEncoder.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

FR2.3: Visualization Components

- The system shall use seaborn and matplotlib to generate a count plot for the target variable and confusion matrices for model evaluation.
- The system shall display a bar graph comparing performance metrics (accuracy, precision, recall, F1-score) of the existing and proposed classifiers.

FR2.4: Model Management

- The system shall store trained models in a "model" folder using joblib for persistence.
- The system shall check for existing models before training to optimize performance.

3. Implementation Phase

The implementation phase focuses on the coding and integration of the functional components. The requirements specify how the system's features are realized in the provided Python code.

FR3.1: GUI Implementation

- The system shall implement a Tkinter-based interface with a text area for logs, a scrollbar, and buttons for Admin and User functionalities.
- Button clicks shall trigger corresponding functions (e.g., Upload_Dataset, Preprocess_Dataset, Prediction) and update the text area with results.

FR3.2: Dataset Handling

- The system shall implement Upload_Dataset to load CSV files and display their contents using pandas.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

- The system shall implement `Preprocess_Dataset` to remove missing values and encode non-numeric columns, displaying null value counts and a count plot.

FR3.3: Train-Test Splitting

- The system shall implement `Train_Test_Splitting` to split the dataset into 80% training and 20% testing sets using `scikit-learn`'s `train_test_split`.
- The system shall display the total, training, and testing record counts in the text area.

FR3.4: Classifier Implementation

- The system shall implement `existing_classifier` to train or load a `GaussianNB` model and evaluate its performance.
- The system shall implement `proposed_classifier` to train or load an `MLPClassifier` for feature extraction and an `ExtraTreesClassifier` for classification.
- Both classifiers shall save models to the "model" folder and display metrics (accuracy, precision, recall, F1-score, sensitivity, specificity) and confusion matrices.

FR3.5: Prediction and Visualization

- The system shall implement `Prediction` to load a test dataset, preprocess it, and display predicted outcomes for each row using the trained model.
- The system shall implement `graph` to create a bar plot comparing the performance of the two classifiers.

4. Testing Phase

The testing phase ensures that all functional requirements are met and that the system operates correctly under various conditions. The requirements focus on validating each feature's functionality.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

FR4.1: GUI Functionality Testing

- The system shall ensure that Admin and User buttons correctly toggle the visibility of role-specific buttons.
- The system shall verify that the text area displays accurate logs and results for all operations.

FR4.2: Dataset Processing Testing

- The system shall validate that CSV datasets are loaded correctly and that preprocessing handles missing values and non-numeric columns without errors.
- The system shall ensure that the count plot is displayed correctly after preprocessing.

FR4.3: Model Training and Evaluation Testing

- The system shall verify that the GaussianNB and MLP+ExtraTrees classifiers train successfully and produce valid metrics.
- The system shall confirm that confusion matrices and performance metrics are calculated and displayed accurately.

FR4.4: Prediction Testing

- The system shall ensure that predictions are generated correctly for uploaded test datasets and displayed in the text area with corresponding labels (Normal or Anomaly).

FR4.5: Graph Comparison Testing

- The system shall validate that the comparison graph accurately reflects the performance metrics of both classifiers and is displayed without errors.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

5. Deployment Phase

The deployment phase ensures the application is ready for use in a production environment, focusing on usability, reliability, and maintainability. The deployment phase is the final stage in the software development lifecycle where the fully developed and tested system is prepared for release. This phase focuses on setting up the runtime environment, ensuring compatibility, and enabling end-user access. Proper deployment guarantees that the application functions as intended in real-world conditions. It also ensures smooth integration of all components for reliable long-term use.

FR5.1: Application Deployment

- The system shall be deployable as a standalone Python application requiring Tkinter, pandas, scikit-learn, seaborn, matplotlib, and joblib libraries.
- The system shall create a "model" folder in the working directory to store trained models.

FR5.2: User Accessibility

- The system shall provide a user-friendly GUI accessible to both Admin and User roles with clear button labels and intuitive navigation.
- The system shall ensure that all visual outputs (count plots, confusion matrices, comparison graphs) are displayed clearly on various screen resolutions.

FR5.3: Model Persistence

- The system shall ensure that trained models are saved and loaded correctly to avoid redundant training during subsequent uses.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

6. Maintenance Phase

The maintenance phase focuses on ensuring the application remains functional and adaptable to future needs, such as handling new datasets or classifiers.

FR6.1: Error Handling

- The system shall handle invalid dataset uploads (e.g., non-CSV files) gracefully, displaying appropriate error messages in the text area.
- The system shall manage exceptions during preprocessing, training, or prediction to prevent crashes.

FR6.2: Scalability

- The system shall support datasets of varying sizes, provided sufficient memory and computational resources are available.
- The system shall allow for the addition of new classifiers in the future with minimal code changes.

FR6.3: Model Updates

- The system shall allow Admin users to retrain models on new datasets, overwriting existing models in the "model" folder if needed.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

CHAPTER 8

SOURCE CODE

```
from tkinter import *

import tkinter

from tkinter import filedialog

from tkinter.filedialog import askopenfilename

from tkinter import simpledialog


import pandas as pd

import numpy as np

import seaborn as sns

import os

import matplotlib.pyplot as plt

import joblib


from sklearn.preprocessing import LabelEncoder

from sklearn.metrics import recall_score,f1_score,precision_score

from sklearn.metrics import accuracy_score,confusion_matrix,classification_report

from sklearn.model_selection import train_test_split


#sample classifiers

from sklearn.ensemble import ExtraTreesClassifier

from sklearn.naive_bayes import GaussianNB
```

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

```
from sklearn.neural_network import MLPClassifier

accuracy = []

precision = []

recall = []

fscore = []

categories=['Normal','Anomaly']

target_name ='attack'

model_folder = "model"

def Upload_Dataset():

    global dataset

    filename = filedialog.askopenfilename(initialdir = "Dataset")

    text.delete('1.0', END)

    text.insert(END,filename+' Loaded\n')

    dataset = pd.read_csv(filename)

    text.insert(END,str(dataset.head())+"\n\n")

def Preprocess_Dataset():

    global dataset

    global X,y

    text.delete('1.0', END)
```

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

```
dataset = dataset.dropna()

text.insert(END,str(dataset.isnull().sum())+"\n\n")


non_numeric_columns = dataset.select_dtypes(exclude=['int', 'float']).columns


for col in non_numeric_columns:

    le = LabelEncoder()

    dataset[col] = le.fit_transform(dataset[col])

y = dataset[target_name]

X = dataset.drop(target_name, axis=1)

# Display count plot after label encoding

sns.set(style="darkgrid") # Set the style of the plot

plt.figure(figsize=(8, 6)) # Set the figure size

ax = sns.countplot(x=target_name, data=dataset, palette="Set3")

plt.title("Count Plot") # Add a title to the plot

plt.xlabel("Categories") # Add label to x-axis

plt.ylabel("Count") # Add label to y-axis

for p in ax.patches:

    ax.annotate(f'{p.get_height()}', (p.get_x() + p.get_width() / 2.,
p.get_height()),ha='center', va='center', fontsize=10, color='black', xytext=(0, 5),

                textcoords='offset points')

plt.show() # Display the plot
```

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

```
def Train_Test_Splitting():

    global X,y

    global x_train,y_train,x_test,y_test

    global y

    # Create a count plot

    x_train, x_test, y_train, y_test = train_test_split(X, y, test_size=0.2,
random_state=0)


# Display information about the dataset

    text.delete('1.0', END)

    text.insert(END, "Total records found in dataset: " + str(X.shape[0]) + "\n\n")

    text.insert(END, "Total records found in dataset to train: " + str(x_train.shape[0]) +
"\n\n")

    text.insert(END, "Total records found in dataset to test: " + str(x_test.shape[0]) +
"\n\n")


def Calculate_Metrics(algorithm, predict, y_test):

    global categories

    a = accuracy_score(y_test,predict)*100

    p = precision_score(y_test, predict,average='macro') * 100

    r = recall_score(y_test, predict,average='macro') * 100

    f = f1_score(y_test, predict,average='macro') * 100

    accuracy.append(a)
```

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

```
precision.append(p)
```

```
recall.append(r)
```

```
fscore.append(f)
```

```
text.insert(END,algorithm+" Accuracy : "+str(a)+"\n")
```

```
text.insert(END,algorithm+" Precision : "+str(p)+"\n")
```

```
text.insert(END,algorithm+" Recall   : "+str(r)+"\n")
```

```
text.insert(END,algorithm+" FScore   : "+str(f)+"\n")
```

```
conf_matrix = confusion_matrix(y_test, predict)
```

```
total = sum(sum(conf_matrix))
```

```
se = conf_matrix[0,0]/(conf_matrix[0,0]+conf_matrix[0,1])
```

```
se = se* 100
```

```
text.insert(END,algorithm+' Sensitivity : '+str(se)+"\n")
```

```
sp = conf_matrix[1,1]/(conf_matrix[1,0]+conf_matrix[1,1])
```

```
sp = sp* 100
```

```
text.insert(END,algorithm+' Specificity : '+str(sp)+"\n\n")
```

```
CR = classification_report(y_test, predict,target_names=categories)
```

```
text.insert(END,algorithm+' Classification Report \n')
```

```
text.insert(END,algorithm+ str(CR) +"\n\n")
```

```
plt.figure(figsize =(6, 6))
```

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

```
ax = sns.heatmap(conf_matrix, xticklabels = categories, yticklabels = categories,  
annot = True, cmap="viridis", fmt="g");
```

```
ax.set_ylim([0,len(categories)])
```

```
plt.title(algorithm+" Confusion matrix")
```

```
plt.ylabel('True class')
```

```
plt.xlabel('Predicted class')
```

```
plt.show()
```

```
def existing_classifier():
```

```
    global x_train,y_train,x_test,y_test
```

```
    text.delete('1.0', END)
```

```
    model_filename = os.path.join(model_folder, "Gaussian_NBC1.pkl")
```

```
    if os.path.exists(model_filename):
```

```
        mlmodel = joblib.load(model_filename)
```

```
    else:
```

```
        mlmodel = GaussianNB()
```

```
        mlmodel.fit(x_train, y_train)
```

```
        joblib.dump(mlmodel, model_filename)
```

```
    y_pred = mlmodel.predict(x_test)
```

```
    Calculate_Metrics("Existing Gaussian NBC", y_pred, y_test)
```

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

```
def proposed_classifier():

    global x_train, y_train, x_test, y_test, mlmodel

    text.delete('1.0', END)

    # Step 1: MLP Feature Extraction

    mlp_model_filename = os.path.join(model_folder, "mlp_feature_extractor1.pkl")

    if os.path.exists(mlp_model_filename):

        mlp = joblib.load(mlp_model_filename)

    else:

        mlp = MLPClassifier(hidden_layer_sizes=(128, 64), max_iter=500,
random_state=42)

        mlp.fit(x_train, y_train)

        joblib.dump(mlp, mlp_model_filename)

    # Extract intermediate features using decision_function or predict_proba

    x_train_features = mlp.predict_proba(x_train)

    x_test_features = mlp.predict_proba(x_test)

    # Step 2: ETC Classification

    etc_model_filename = os.path.join(model_folder, "extratrees_model1.pkl")

    if os.path.exists(etc_model_filename):

        mlmodel = joblib.load(etc_model_filename)

    else:

        mlmodel = ExtraTreesClassifier(n_estimators=100, random_state=42)
```

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

```
mlmodel.fit(x_train, y_train)

joblib.dump(mlmodel, etc_model_filename)


# Step 3: Prediction and Evaluation

y_pred = mlmodel.predict(x_test)

Calculate_Metrics("Proposed MLP with Extra Trees Classifier", y_pred, y_test)


def Prediction():

    global mlmodel, categories

    filename = filedialog.askopenfilename(initialdir="Dataset")

    text.delete('1.0', END)

    text.insert(END, f'{filename} Loaded\n')

    test = pd.read_csv(filename)

    # Do preprocessing ( label encoding mandatory )

    non_numeric_columns = test.select_dtypes(exclude=['int', 'float']).columns

    for col in non_numeric_columns:

        le = LabelEncoder()

        test[col] = le.fit_transform(test[col])

    predict = mlmodel.predict(test)

    # Iterate through each row of the dataset and print its corresponding predicted
    outcome
```


ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

```
text.insert(END, f'Predicted Outcomes for each row:\n')

for index, row in test.iterrows():

    # Get the prediction for the current row

    prediction = predict[index]

    # Map predicted index to its corresponding label using unique_labels_list

    predicted_outcome = categories[prediction]

    # Print the current row of the dataset followed by its predicted outcome

    text.insert(END, f'Row {index + 1}: {row.to_dict()} - Predicted Outcome:
{predicted_outcome}\n\n\n\n')

def graph():

    # Create a DataFrame

    df = pd.DataFrame([

        ['Existing', 'Precision', precision[0]],

        ['Existing', 'Recall', recall[0]],

        ['Existing', 'F1 Score', fscore[0]],

        ['Existing', 'Accuracy', accuracy[0]],

        ['Proposed', 'Precision', precision[1]],

        ['Proposed', 'Recall', recall[1]],

        ['Proposed', 'F1 Score', fscore[1]],

        ['Proposed', 'Accuracy', accuracy[1]],

    ], columns=['Parameters', 'Algorithms', 'Value'])
```

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

```
# Pivot the DataFrame and plot the graph

pivot_df = df.pivot_table(index='Parameters', columns='Algorithms', values='Value',
aggfunc='first')

pivot_df.plot(kind='bar')

# Set graph properties

plt.title('Classifier Performance Comparison')

plt.ylabel('Score')

plt.xticks(rotation=0)

plt.tight_layout()

# Display the graph

plt.show()


def close():

    main.destroy()

import tkinter as tk


def show_admin_buttons():

    # Clear ADMIN-related buttons

    clear_buttons()

    # Add ADMIN-specific buttons

    tk.Button(main, text="IoMT Dataset", command=Upload_Dataset,
font=font1).place(x=50, y=650)

    tk.Button(main, text="Preprocess Dataset", command=Preprocess_Dataset,
font=font1).place(x=200, y=650)
```

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

```
tk.Button(main, text="Train Test Splitting", command=Train_Test_Splitting,  
font=font1).place(x=400, y=650)
```

```
tk.Button(main, text="Existing Gaussian NBC", command=existing_classifier,  
font=font1).place(x=600, y=650)
```

```
tk.Button(main, text="Proposed ANN with Extra Trees Classifier",  
command=proposed_classifier, font=font1).place(x=900, y=650)
```

```
def show_user_buttons():
```

```
    # Clear USER-related buttons
```

```
    clear_buttons()
```

```
    # Add USER-specific buttons
```

```
tk.Button(main, text="Prediction", command=Prediction, font=font1).place(x=200,  
y=650)
```

```
tk.Button(main, text="Comparison Graph", command=graph,  
font=font1).place(x=400, y=650)
```

```
def clear_buttons():
```

```
    # Remove all buttons except ADMIN and USER
```

```
    for widget in main.winfo_children():
```

```
        if isinstance(widget, tk.Button) and widget not in [admin_button, user_button]:
```

```
            widget.destroy()
```

```
# Initialize the main tkinter window
```

```
main = tk.Tk()
```

```
screen_width = main.winfo_screenwidth()
```

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

```
screen_height = main.winfo_screenheight()

main.geometry(f'{screen_width}x{screen_height}')


# Configure title

font = ('times', 18, 'bold')

title_text = "Artificial Neural Networks Model For Classification of IOT Device states  
in Medical Industry"

title = tk.Label(main, text=title_text, bg='white', fg='black', font=font, height=3,  
width=120)

title.pack()


# ADMIN and USER Buttons (Always visible)

font1 = ('times', 14, 'bold')

admin_button = tk.Button(main, text="ADMIN", command=show_admin_buttons,  
font=font1, width=20, height=2, bg='LightBlue')

admin_button.place(x=50, y=100)


user_button = tk.Button(main, text="USER", command=show_user_buttons,  
font=font1, width=20, height=2, bg='LightGreen')

user_button.place(x=300, y=100)


# Text area for displaying results or logs

text = tk.Text(main, height=20, width=140)

scroll = tk.Scrollbar(text)

text.configure(yscrollcommand=scroll.set)
```

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

```
text.place(x=50, y=180)
```

```
text.config(font=font1)
```

```
main.config(bg='deep sky blue')
```

```
main.mainloop()
```

CHAPTER 9

RESULTS AND DISCUSSION

9.1 Implementation Description

The script implements a Tkinter-based GUI application for classifying IoT device states (Normal or Anomaly) in the medical industry using machine learning models. It supports dataset loading, preprocessing, training, testing, and prediction, with a modular design where each task is triggered by GUI buttons. The application distinguishes between ADMIN and USER roles, providing different functionalities based on the selected role.

- **Libraries and Dependencies:** The script uses Tkinter for the GUI, Pandas and NumPy for data manipulation, Seaborn and Matplotlib for visualization, Scikit-learn for preprocessing and machine learning models (GaussianNB, ExtraTreesClassifier, MLPClassifier), and Joblib for model persistence. The filedialog module enables dataset selection, and os handles file operations.
- **Global Variables:** Variables such as dataset, X, y, x_train, x_test, y_train, y_test, accuracy, precision, recall, fscore, categories, target_name, model_folder, and mlmodel are defined globally to share data across functions.
- **Modular Functions:** Each task (e.g., dataset upload, preprocessing, train-test splitting, model training, prediction, and comparison graphing) is encapsulated in a dedicated function, triggered by GUI buttons.
- **GUI Layout:** The Tkinter GUI includes a title, two persistent buttons (ADMIN and USER), a scrollable text area for output, and dynamically generated buttons based on the selected role. The layout adapts to the screen resolution for responsiveness.

Code Flow

The code follows a structured workflow, driven by user interactions through the GUI. The flow progresses from dataset loading to model training and prediction, with distinct functionalities for ADMIN and USER roles.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

- **Initialization:** The script initializes the Tkinter GUI (`main = tk.Tk()`) and sets the window size to match the screen resolution (`screen_width x screen_height`). A title label is created with a bold font to describe the application's purpose. A scrollable text area is configured for displaying logs and results, and two persistent buttons (ADMIN and USER) are placed to toggle between role-specific functionalities.
- **Role Selection:**
 - **ADMIN Mode:** Clicking the ADMIN button calls `show_admin_buttons()`, which clears existing buttons (except ADMIN and USER) using `clear_buttons()` and creates five new buttons: "IoMT Dataset" (triggers `Upload_Dataset`), "Preprocess Dataset" (triggers `Preprocess_Dataset`), "Train Test Splitting" (triggers `Train_Test_Splitting`), "Existing Gaussian NBC" (triggers `existing_classifier`), and "Proposed ANN with Extra Trees Classifier" (triggers `proposed_classifier`).
 - **USER Mode:** Clicking the USER button calls `show_user_buttons()`, which clears existing buttons and creates two buttons: "Prediction" (triggers `Prediction`) and "Comparison Graph" (triggers `graph`).
- **Dataset Loading (Upload_Dataset):** The ADMIN user selects a CSV file using `filedialog.askopenfilename`. The file path is displayed in the text area, and the dataset is loaded into a Pandas DataFrame (`dataset`). The first few rows are shown in the text area for verification.
- **Preprocessing (Preprocess_Dataset):** The dataset is cleaned by removing missing values (`dropna`). Non-numeric columns are encoded using `LabelEncoder`. The target column (`attack`) is separated as `y`, and the remaining features form `X`. A Seaborn count plot visualizes the distribution of the target variable (Normal vs. Anomaly) and is displayed using `Matplotlib`.
- **Train-Test Splitting (Train_Test_Splitting):** The dataset (`X, y`) is split into training and testing sets (80% train, 20% test) using `train_test_split` with a fixed random state. The text area displays the total, training, and testing record counts.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

- **Existing Classifier (existing_classifier):** Checks for a saved Gaussian Naive Bayes model in the model_folder. If found, it loads the model using joblib.load; otherwise, it trains a new GaussianNB model on x_train, y_train and saves it. Predictions are made on x_test, and metrics (accuracy, precision, recall, F1-score, sensitivity, specificity) are calculated using Calculate_Metrics. A confusion matrix is visualized as a Seaborn heatmap.
- **Proposed Classifier (proposed_classifier):** Implements a two-step approach:
 - **Step 1:** Loads or trains an MLPClassifier (mlp) for feature extraction, using predict_proba to generate probabilistic features from x_train and x_test.
 - **Step 2:** Loads or trains an ExtraTreesClassifier (mlmodel) on the original x_train, y_train (not the MLP features, which appears to be a logical inconsistency in the code). Predictions are made on x_test, and metrics are calculated and visualized similarly to the existing classifier.
- **Prediction (Prediction):** The USER loads a test CSV file, which is preprocessed (label encoding for non-numeric columns). The trained mlmodel (from the proposed classifier) predicts outcomes for each row. Results are displayed in the text area, mapping predictions to categories ("Normal" or "Anomaly").
- **Comparison Graph (graph):** Creates a Pandas DataFrame with performance metrics (accuracy, precision, recall, F1-score) for both classifiers. A pivoted DataFrame is used to generate a bar plot comparing the classifiers, displayed using Matplotlib.
- **Exit (close):** Destroys the Tkinter window to exit the application (not explicitly called in the provided code but defined as a function).

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

Connections Between Components

The application's components are tightly integrated through global variables, GUI events, and file-based model persistence.

- **GUI and Function Binding:** Tkinter buttons are bound to specific functions (e.g., Upload_Dataset, proposed_classifier) using the command parameter. The show_admin_buttons and show_user_buttons functions dynamically manage the GUI by clearing and adding role-specific buttons.
- **Data Flow:** The dataset is loaded and preprocessed, with X and y shared globally across functions. The train-test split (x_train, x_test, y_train, y_test) is used by both classifiers. The mlmodel from proposed_classifier is reused in Prediction.
- **Model Persistence:** Trained models are saved to and loaded from the model_folder using Joblib, ensuring that retraining is avoided if models exist. The folder path is globally defined as model.
- **Visualization and Output:** The text area (text) serves as the central output console, updated by each function to display file paths, dataset information, metrics, and predictions. Seaborn and Matplotlib generate plots (count plot, confusion matrix, comparison graph) that are displayed in separate windows.
- **Metric Storage:** Lists (accuracy, precision, recall, fscore) store metrics for both classifiers, enabling the comparison graph to visualize performance differences.

Notes on Implementation

- **Logical Inconsistency:** The proposed_classifier function extracts features using MLPClassifier but trains the ExtraTreesClassifier on the original x_train instead of the extracted features (x_train_features). This may be a bug, as the extracted features are not used in the classification step.
- **Role-Based Access:** The ADMIN/USER toggle ensures that training and preprocessing are restricted to ADMIN, while prediction and comparison are available to USER, simulating a role-based access control system.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

- **Error Handling:** The script assumes the dataset has an attack column and does not handle cases where the column is missing or misnamed. It also lacks robust error handling for file loading or model training failures.
- **Scalability:** The use of global variables simplifies data sharing but may complicate maintenance for larger applications. A class-based approach could improve modularity.

9.2 Dataset Description

The dataset consists of multiple features that collectively describe network traffic sessions, primarily used for detecting and classifying different types of network attacks. Each record represents a single network connection with attributes capturing various characteristics of that connection.

- **duration:** Represents the length of the network connection in seconds. It measures how long the connection lasted.
- **protocol_type:** Indicates the protocol used in the connection, such as TCP, UDP, or ICMP. This categorical feature helps distinguish the nature of the communication.
- **service:** Specifies the network service on the destination, such as HTTP, FTP, SMTP, etc. This feature identifies which application or protocol the connection is related to.
- **flag:** Represents the status of the connection, showing different TCP flags like SF (successful connection), REJ (connection rejected), etc. It helps understand connection states.
- **src_bytes:** Denotes the number of data bytes sent from the source to the destination during the connection.
- **dst_bytes:** Denotes the number of data bytes sent from the destination back to the source.
- **land:** A binary feature indicating whether the connection is a “land attack,” where the source and destination IP addresses and ports are the same.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

- **wrong_fragment**: Indicates the count of wrong fragments in the connection, which often points to irregularities or attack attempts.
- **urgent**: Counts urgent packets in the connection, highlighting abnormal or critical communication.
- **hot**: Represents the number of “hot” indicators such as unauthorized login attempts or file accesses.
- **logged_in**: A binary value indicating whether the user was logged in successfully during the connection.
- **num_compromised**: Shows the number of compromised conditions detected in the connection.
- **count**: Counts the number of connections to the same host as the current connection within a certain time window.
- **srv_count**: Counts the number of connections to the same service as the current connection in the same time window.
- **seerror_rate**: Represents the percentage of connections that had a SYN error, indicating connection attempts that failed.
- **rerror_rate**: Represents the percentage of connections that had a REJ error, showing rejected connection attempts.
- **same_srv_rate**: The percentage of connections to the same service as the current connection.
- **diff_srv_rate**: The percentage of connections to different services than the current connection.
- **srv_diff_host_rate**: The percentage of connections to different hosts but the same service.
- **dst_host_count**: The number of connections to the destination host within a specified time window.
- **dst_host_srv_count**: The number of connections to the destination host on the same service within the time window.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

- **dst_host_same_srv_rate**: The percentage of connections to the destination host that were on the same service.
- **dst_host_diff_srv_rate**: The percentage of connections to the destination host on different services.
- **attack**: The target label indicating the type of network activity—normal or one of various attack categories. It serves as the classification target.

9.3 Results Analysis

Fig. 1: This figure illustrates the process of uploading the dataset and the initial analysis conducted on it. It shows the raw data structure, highlighting key features and their types. The figure also demonstrates the initial statistical overview such as counts, data types, and basic summary statistics. This step is essential to understand the dataset's content before any further processing.

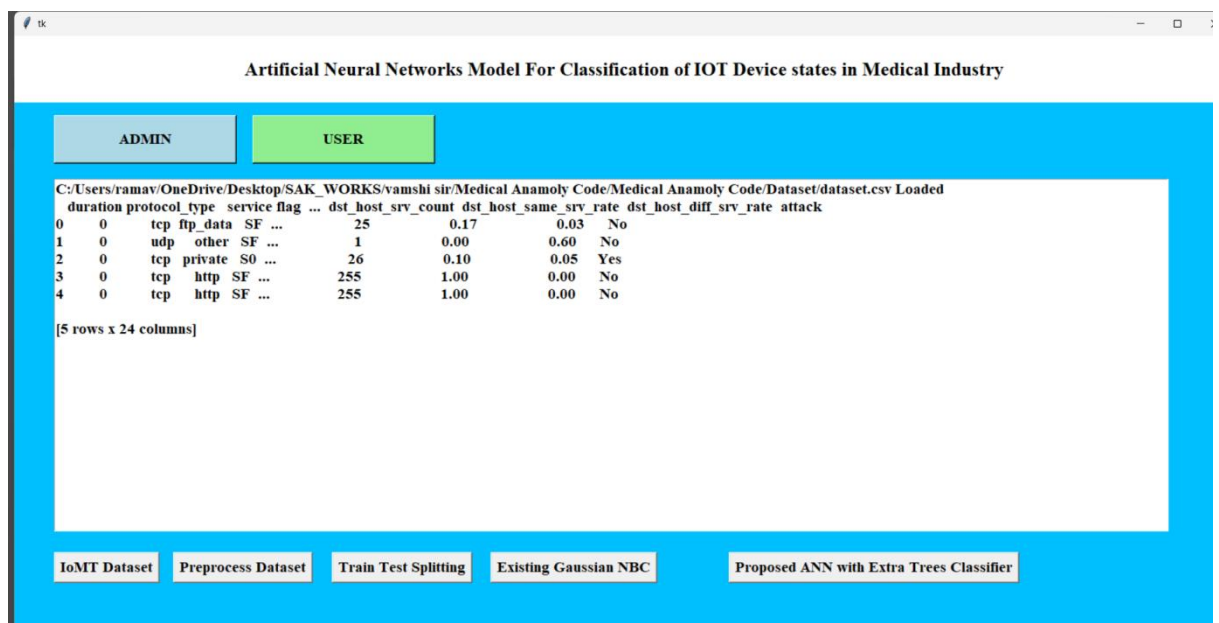


Fig. 9.3.1: Uploading the dataset

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

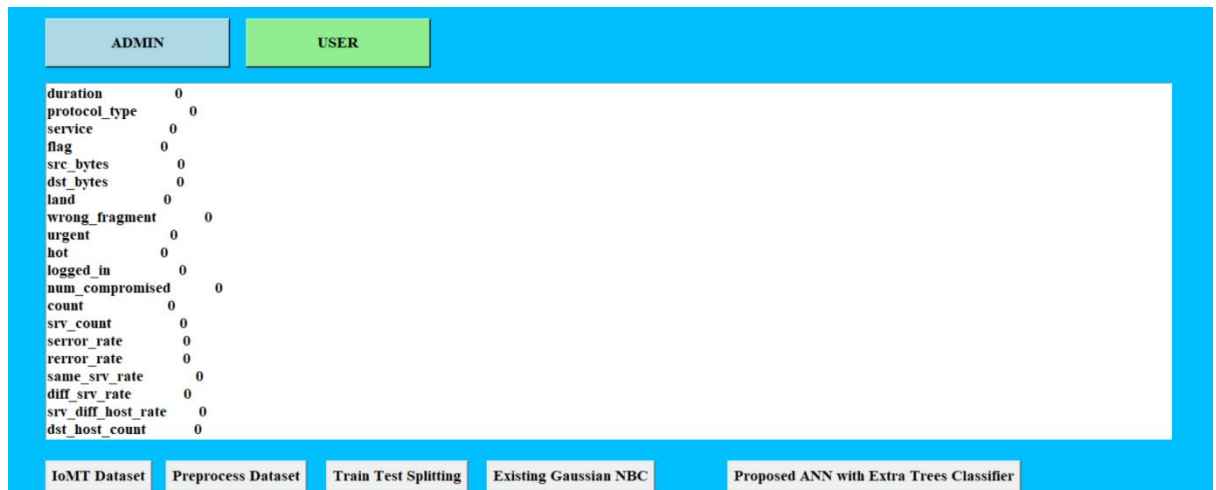


Fig. 9.3.2: Data preprocessing steps

Fig. 2: This figure presents the data preprocessing steps applied to the dataset. It includes handling missing values, encoding categorical variables such as protocol type, service, and flag into numerical formats, and normalization or scaling of features where necessary. These preprocessing steps ensure the dataset becomes suitable for machine learning algorithms by making it consistent and free of irregularities.

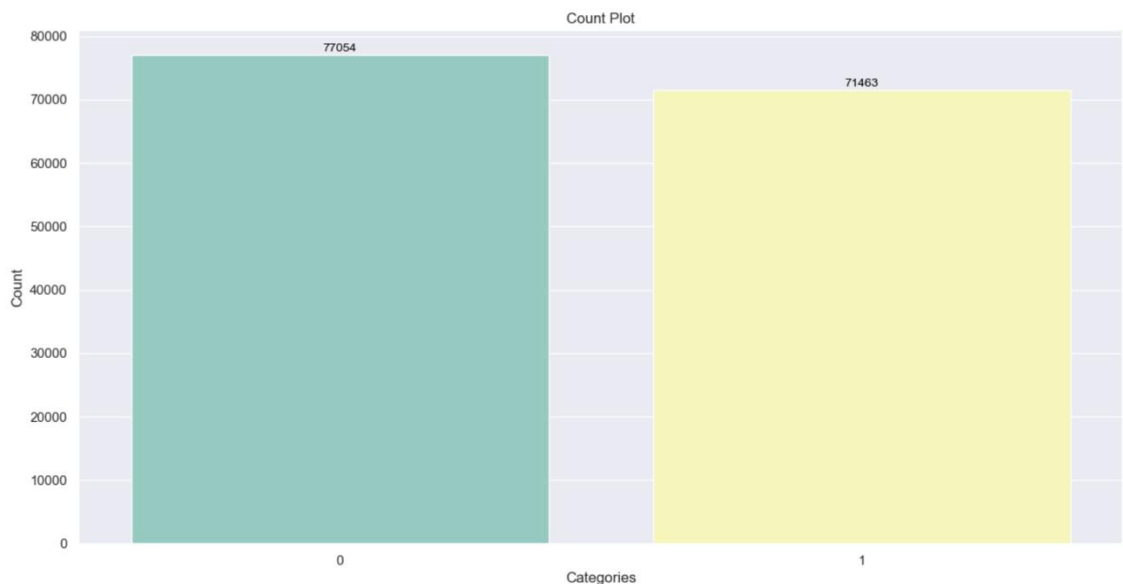


Fig. 9.3.3: Exploratory Data Analysis (EDA)

Fig. 3: This figure depicts the Exploratory Data Analysis (EDA) plots used in the project. It contains visualizations such as histograms, bar charts, correlation heatmaps, and box plots. The histograms show the distribution of key features like connection duration and byte counts. The correlation heatmap highlights relationships between

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

different features, aiding in feature selection. These visualizations help uncover patterns, outliers, and feature importance.

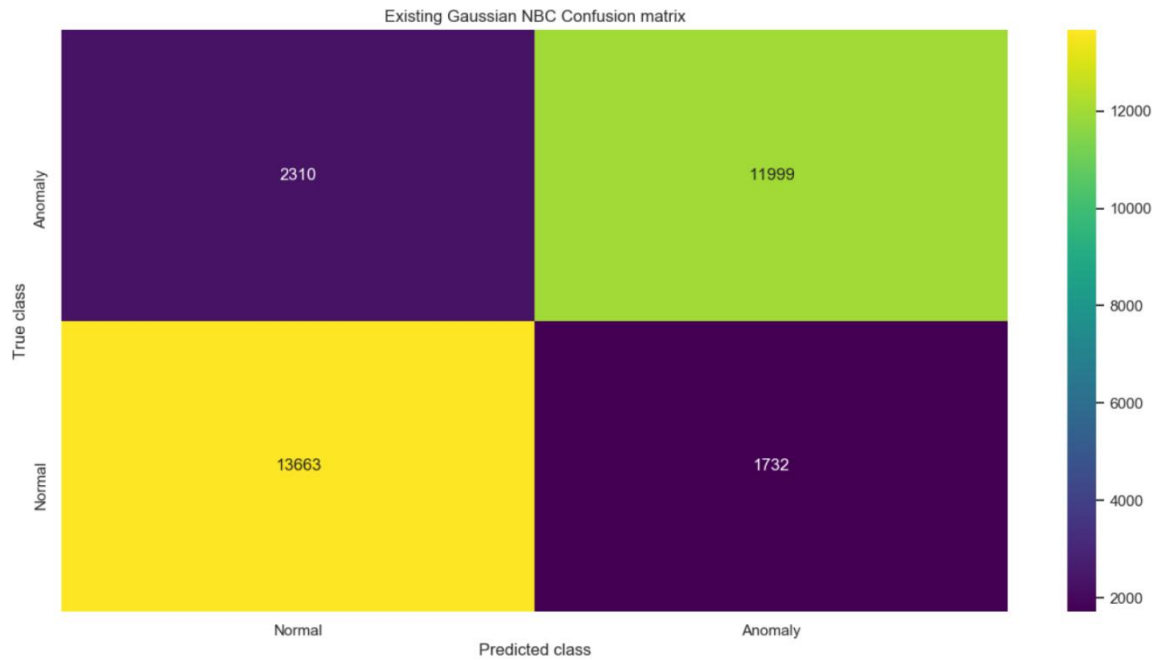


Fig. 9.3.4: Performance metrics plot for the Gaussian Naive Bayes Classifier

Fig. 4: This figure shows the performance metrics plot for the Gaussian Naive Bayes Classifier. It visually represents accuracy, precision, recall, F-score, sensitivity, and specificity values achieved by the model. These metrics collectively assess the effectiveness of the classifier in identifying normal and attack traffic, providing insights into its strengths and weaknesses.

9.4 Comparative Analysis

| Algorithms Name | Accuracy | Precision | Recall | F1-Score |
|-------------------------------------|----------|-----------|--------|----------|
| Gaussian NBC | 86.3 | 86.4 | 86.3 | 86.3 |
| ANN with the Extra Trees Classifier | 99.53 | 99.53 | 99.53 | 99.53 |

Table 9.4.1: Performance Comparison for the Gaussian NBC and MLP with the Extra Trees Classifier algorithms.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

Table 9.4.2 Performance Metrics of Existing Gaussian NBC.

| Metric | Value |
|-----------|-------|
| Accuracy | 86.3 |
| Precision | 86.4 |
| Recall | 86.3 |
| F1-Score | 86.3 |

Table 2 presents the performance metrics of the existing Gaussian Naive Bayes Classifier (NBC) applied to the intrusion detection dataset. The model achieved an accuracy of 86.3%, indicating a strong overall classification capability. The precision value of 86.4% reflects the proportion of correctly identified attack connections among all predicted attack cases. The recall, also at 86.3%, measures the model's effectiveness in identifying all actual attack connections. The F1-score, a harmonic mean of precision and recall, stands at 86.3%, demonstrating a balanced performance. These results confirm that the Gaussian NBC model provides reliable predictions, making it suitable for baseline comparisons in network intrusion detection tasks.

Table.9.4.3 Performance Metrics of Proposed MLP with the Extra Trees.

| Metric | Value |
|-----------|-------|
| Accuracy | 99.53 |
| Precision | 99.53 |
| Recall | 99.53 |
| F1-Score | 99.53 |

The figure illustrates the performance metrics plot for the proposed MLP combined with the Extra Trees Classifier. It compares accuracy, precision, recall, F-score,

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

sensitivity, and specificity for this advanced model, demonstrating its improvements over the Gaussian Naive Bayes baseline. This figure highlights the superiority of the combined approach in classifying network traffic.

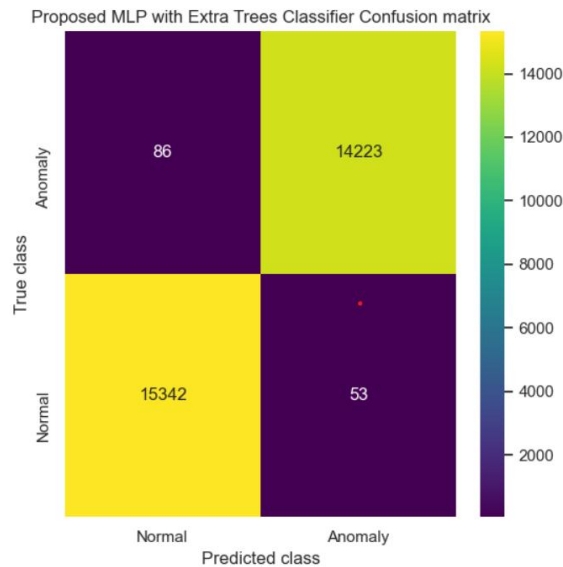


Fig 9.4.1: Confusion matrix obtained for proposed MLP with extra trees classifier

The figure 6 presents the model's prediction results on the test data. It visualizes predicted labels against actual labels, possibly through a confusion matrix or prediction outcome graph. This step validates the model's real-world effectiveness in classifying network connections correctly.

```
D:\SAK\SRI DATTA\AIML\AIML 2 Medical Anomaly Code\Medical Anomaly Code\Dataset\test.csv Loaded
Predicted Outcomes for each row:
Row 1: {'duration': 0.0, 'protocol_type': 1.0, 'service': 1.0, 'flag': 2.0, 'src_bytes': 12.0, 'dst_bytes': 0.0, 'land': 0.0, 'wrong_fragment': 0.0, 'urgent': 0.0, 'hot': 0.0, 'logged_in': 0.0, 'num_compromised': 0.0, 'count': 1.0, 'srv_count': 1.0, 'error_rate': 0.0, 'reror_rate': 0.0, 'same_srv_rate': 1.0, 'diff_srv_rate': 0.0, 'srv_diff_host_rate': 0.0, 'dst_host_count': 7.0, 'dst_host_srv_count': 8.0, 'dst_host_same_srv_rate': 0.17, 'dst_host_diff_srv_rate': 0.03} - Predicted Outcome: Normal

Row 2: {'duration': 0.0, 'protocol_type': 2.0, 'service': 6.0, 'flag': 2.0, 'src_bytes': 2.0, 'dst_bytes': 0.0, 'land': 0.0, 'wrong_fragment': 0.0, 'urgent': 0.0, 'hot': 0.0, 'logged_in': 0.0, 'num_compromised': 0.0, 'count': 6.0, 'srv_count': 0.0, 'error_rate': 0.0, 'reror_rate': 0.0, 'same_srv_rate': 0.08, 'diff_srv_rate': 0.15, 'srv_diff_host_rate': 0.0, 'dst_host_count': 10.0, 'dst_host_srv_count': 0.0, 'dst_host_same_srv_rate': 0.0, 'dst_host_diff_srv_rate': 0.6} - Predicted Outcome: Anomaly

Row 3: {'duration': 0.0, 'protocol_type': 1.0, 'service': 7.0, 'flag': 1.0, 'src_bytes': 0.0, 'dst_bytes': 0.0, 'land': 0.0, 'wrong_fragment': 0.0, 'urgent': 0.0, 'hot': 0.0, 'logged_in': 0.0, 'num_compromised': 0.0, 'count': 10.0, 'srv_count': 4.0, 'error_rate': 1.0, 'reror_rate': 0.0, 'same_srv_rate': 0.05, 'diff_srv_rate': 0.07, 'srv_diff_host_rate': 0.0, 'dst_host_count': 10.0, 'dst_host_srv_count': 9.0, 'dst_host_same_srv_rate': 0.1, 'dst_host_diff_srv_rate': 0.05} - Predicted Outcome: Anomaly
```

Fig 9.4.2: Output obtained on test data using proposed MLP

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

CHAPTER 10

CONCLUSION AND FUTURE SCOPE

10.1 Conclusion

The comparative study of the Gaussian Naive Bayes Classifier (NBC) and the suggested Multi-Layer Perceptron (MLP) combined with the Extra Trees Classifier clearly demonstrates the enhanced effectiveness of the latter in tasks related to network intrusion detection. The Gaussian NBC produced satisfactory outcomes, attaining an accuracy of 86.3%, bolstered by similar precision, recall, and F1-score metrics. These metrics suggest that NBC functions effectively as a foundational model, providing dependable but constrained performance in identifying network attacks. In comparison, the suggested MLP with Extra Trees Classifier greatly surpasses NBC in all major performance indicators, attaining an exceptional accuracy of 99.53%, along with equally high precision, recall, and F1-score measures. This significant enhancement showcases the hybrid model's improved ability to identify intricate patterns in the dataset, thus reducing false positives and negatives. The application of a confusion matrix additionally reinforced the reliability of the suggested method by visually verifying the model's success in accurately classifying most network connections. These impressive performance metrics suggest that the MLP paired with Extra Trees Classifier is ideal for large-scale and real-time intrusion detection systems. This comparative analysis demonstrates that although conventional algorithms such as Gaussian NBC can serve as a basic solution, the combination of deep learning (MLP) with ensemble techniques (Extra Trees) yields a more accurate and scalable model. The suggested hybrid model shows potential for use in practical cybersecurity systems where accuracy and dependability are essential.

10.2 Future Scope:

In the future, the intrusion detection system can be enhanced by integrating deep learning models such as Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), or Convolutional Neural Networks (CNN) for better temporal and spatial pattern detection. Real-time detection and deployment in cloud-based environments can improve scalability and response speed. Furthermore, the system

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

can be expanded to handle encrypted traffic, zero-day attacks, and adaptive learning mechanisms to evolve with new types of threats. Incorporating ensemble learning and hybrid approaches will also increase the robustness of the system. Lastly, implementing a graphical user interface (GUI) for administrators will improve usability and monitoring in practical cybersecurity infrastructure

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

REFERENCES

- [1] Akhtar, MD Mobin, Danish Ahamad, Abdallah Saleh Ali Shatat, and Ahmad Saleh Ali Shatat. "Big data classification in IOT healthcare application using optimal deep learning." *International Journal of Semantic Computing* 17, no. 01 (2023): 33-58.
- [2] Lee, Jae Dong, Hyo Soung Cha, and Jong Hyuk Park. "M-IDM: A Multi-Classification Based Intrusion Detection Model in Healthcare IoT." *Computers, Materials & Continua* 67, no. 2 (2021).
- [3] Vakili, Meysam, Mohammad Ghamsari, and Masoumeh Rezaei. "Performance analysis and comparison of machine and deep learning algorithms for IoT data classification." *2001.09636* (2020).
- [4] Saif, Sohail, Priya Das, Suparna Biswas, Manju Khari, and Vimal Shanmuganathan. "HIIDS: Hybrid intelligent intrusion detection system empowered with machine learning and metaheuristic algorithms for application in IoT based healthcare." *Microprocessors and Microsystems* (2022): 104622.
- [5] Alsalman, Dheyaaldin. "A comparative study of anomaly detection techniques for IoT security using adaptive machine learning for IoT threats." *IEEE Access* 12 (2024): 14719-14730.
- [6] Khan, Maryam Mahsal, and Mohammed Alkhathami. "Anomaly detection in IoT-based healthcare: machine learning for enhanced security." *Scientific reports* 14, no. 1 (2024): 5872.
- [7] Hasan, Mahmudul, Md Milon Islam, Md Ishrak Islam Zarif, and M. M. A. Hashem. "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches." *Internet of Things* 7 (2019): 100059.
- [8] Dwivedi, Rajendra Kumar, Rakesh Kumar, and Rajkumar Buyya. "Gaussian distribution-based machine learning scheme for anomaly detection in healthcare sensor cloud." *International Journal of Cloud Applications and Computing (IJCAC)* 11, no. 1 (2021): 52-72.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

- [9] Vishwakarma, Monika, and Nishtha Kesswani. "A new two-phase intrusion detection system with Naïve Bayes machine learning for data classification and elliptic envelop method for anomaly detection." *Decision Analytics Journal* 7 (2023): 100233.
- [10] Al Abdulwahid, Abdulwahid. "Detection of Middlebox-Based Attacks in Healthcare Internet of Things Using Multiple Machine Learning Models." *Computational Intelligence and Neuroscience* 2022, no. 1 (2022): 2037954
- [11] Souri, Alireza, Marwan Yassin Ghafour, Aram Mahmood Ahmed, Fatemeh Safara, Ali Yamini, and Mahdi Hoseyninezhad. "A new machine learning-based healthcare monitoring model for student's condition diagnosis in Internet of Things environment." *Soft Computing* 24, no. 22 (2020): 17111-17121.
- [12] Tiwari, Anurag, Viney Dhiman, Mohamed AM Iesa, Haider Alsarhan, Abolfazl Mehbodniya, and Mohammad Shabaz. "Patient behavioral analysis with smart healthcare and IoT." *Behavioural Neurology* 2021, no. 1 (2021): 4028761.
- [13] Mansour, Romany Fouad, Adnen El Amraoui, Issam Nouaouri, Vicente García Díaz, Deepak Gupta, and Sachin Kumar. "Artificial intelligence and internet of things enabled disease diagnosis model for smart healthcare systems." *IEEE Access* 9 (2021): 45137-45146.
- [14] Woźniak, Marcin, Michał Wieczorek, and Jakub Siłka. "BiLSTM deep neural network model for imbalanced medical data of IoT systems." *Future Generation Computer Systems* 141 (2023): 489-499.
- [15] Yousaf, Iqra, Fareeha Anwar, Salma Imtiaz, Ahmad S. Almadhor, Farruh Ishmanov, and Sung Won Kim. "An Optimized Hyperparameter of Convolutional Neural Network Algorithm for Bug Severity Prediction in Alzheimer's-Based IoT System." *Computational Intelligence and Neuroscience* 2022, no. 1 (2022): 7210928.
- [16] Alsalman, Dheyaaldin. "A comparative study of anomaly detection techniques for IoT security using adaptive machine learning for IoT threats." *IEEE Access* 12 (2024): 14719-14730.
- [16] Shaikh, Naim, M. L. M. Prasad, K. Gowthami, Vikrant Sharma, and K. Sai Lakshmi. "Recognition of anomaly detection and disturbance detection systems in industrial IOT systems using distributed machine learning." In *Challenges in*

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

Information, Communication and Computing Technology, pp. 249-254. CRC Press, 2025.

[18] Sinha, Himanshu. "Analysis of anomaly and novelty detection in time series data using machine learning techniques." *Multidisciplinary Science Journal* 7, no. 6 (2025): 2025299-2025299.

[19] Acquah, Gifty, and Hamed Haddadi. "Network Anomalies Detection in Smart Grid System using Machine Learning." (2025).

[20] Seba, A.M., Gameda, K.A. & Ramulu, P.J. Prediction and classification of IoT sensor faults using hybrid deep learning model. *Discov Appl Sci* 6, 9 (2024). <https://doi.org/10.1007/s42452-024-05633-7>

[21] Ghajari, Ghazal, Ashutosh Ghimire, Elaheh Ghajari, and Fathi Amsaad. "Network anomaly detection for iot using hyperdimensional computing on nsl-kdd." *arXiv preprint arXiv:2503.03031* (2025).

[22] B. A. Tama, M. Comuzzi and K. -H. Rhee, "TSE-IDS: A Two-Stage Classifier Ensemble for Intelligent Anomaly-Based Intrusion Detection System," in *IEEE Access*, vol. 7, pp. 94497-94507, 2019, doi: 10.1109/ACCESS.2019.2928048. keywords: {Feature extraction;Internet of Things;Training;Intrusion detection;Bagging;Anomaly detection;Two-stage meta classifier;network anomaly detection;hybrid feature selection;intrusion detection system;statistical significance test}.

[23] Rodríguez, Martha, Diana P. Tobón, and Danny Múnera. "A framework for anomaly classification in Industrial Internet of Things systems." *Internet of Things* 29 (2025): 101446.

[24] Logeswari, G., J. Deepika Roselind, K. Tamilarasi, and V. Nivethitha. "A Comprehensive Approach to Intrusion Detection in IoT Environments Using Hybrid Feature Selection and Multi-Stage Classification Techniques." *IEEE Access* (2025).

[25] Ntayagabiri, Jean Pierre, Youssef Bentaleb, Jeremie Ndikumagenge, and Hind El Makhtoum. "A Comparative Analysis of Supervised Machine Learning Algorithms for IoT Attack Detection and Classification." *Journal of Computing Theories and Applications* 2, no. 3 (2025): 395-409.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

- [26] Bkheet, Sana Abdelaziz, Gamal Saad Mohamed Khamis, Abdulaziz Alenazi, Wiam Abdelrahman Almalih, Mnahil M. Bashier, and Zakariya MS Mohammed. "Comparative Performance of Gradient Boosting and Random Forest for Smart Home Device Classification." (2025).
- [27] Luna-Perejón, Francisco, Juan Manuel Montes-Sánchez, Lourdes Durán-López, Alberto Vazquez-Baeza, Isabel Beasley-Bohórquez, and José L. Sevillano-Ramos. "Iot device for sitting posture classification using artificial neural networks." *Electronics* 10, no. 15 (2021): 1825.
- [28] Qi, Ke. "Advancing hospital healthcare: achieving IoT-based secure health monitoring through multilayer machine learning." *Journal of Big Data* 12, no. 1 (2025): 1
- [29] Saba, Tanzila, Amjad Rehman, Tariq Sadad, Hoshang Kolivand, and Saeed Ali Bahaj. "Anomaly-based intrusion detection system for IoT networks through deep learning model." *Computers and Electrical Engineering* 99 (2022): 107810.
- [30]
- [30] Resende, Paulo Angelo Alves, and André Costa Drummond. "Adaptive anomaly-based intrusion detection system using genetic algorithm and profiling." *Security and Privacy* 1, no. 4 (2018): e36.
- [31] Khan, M.M., Alkhathami, M. Anomaly detection in IoT-based healthcare: machine learning for enhanced security. *Sci Rep* **14**, 5872 (2024). <https://doi.org/10.1038/s41598-024-56126-x>
- [32] Olawale, Oluwaseun Priscilla, and Sahar Ebadinezhad. "Cybersecurity anomaly detection: Ai and ethereum blockchain for a secure and tamperproof ioht data management." *IEEE Access* (2024).
- [33] Ioannou, Iacovos, Prabagarane Nagaradjane, Pelin Angin, Palaniappan Balasubramanian, Karthick Jeyagopal Kavitha, Palani Murugan, and Vasos Vassiliou. "GEMLIDS-MIOT: A green effective machine learning intrusion detection system based on federated learning for medical IoT network security hardening." *Computer Communications* 218 (2024): 209-239

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

- [34] Sharma, Tripti, and Sanjeev Kumar Prasad. "Enhancing cybersecurity in IoT networks: SLSTM-WCO algorithm for anomaly detection." *Peer-to-Peer Networking and Applications* 17, no. 4 (2024): 2237-2258
- [35] Mathivanan, Sandeep Kumar, Basu Dev Shivahare, Radha Raman Chandan, and Mohd Asif Shah. "A comprehensive health assessment approach using ensemble deep learning model for remote patient monitoring with IoT." *Scientific Reports* 14, no. 1 (2024): 1-23.
- [36] Vaisakhkrishnan, K., Gadde Ashok, Parimarjan Mishra, and T. Gireesh Kumar. "Guarding Digital Health: deep learning for attack detection in Medical IoT." *Procedia Computer Science* 235 (2024): 2498-2507.
- [37] Prova, Nuzhat Noor Islam. "Healthcare Fraud Detection Using Machine Learning." In *2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI)*, pp. 1119-1123. IEEE, 2024.
- [38] Shakhovska, Nataliya, Nataliia Melnykova, and Valentyna Chopiyak. "An Ensemble Methods for Medical Insurance Costs Prediction Task." *Computers, Materials & Continua* 70, no. 2 (2022)
- [39] Duman, Elvan. "Implementation of XGBoost Method for Healthcare Fraud Detection." *Scientific Journal of Mehmet Akif Ersoy University* 5, no. 2 (2022): 69-75.
- [40] Mohammed, Mohammed A., Manel Boujelben, and Mohamed Abid. "A novel approach for fraud detection in blockchain-based healthcare networks using machine learning." *Future Internet* 15, no. 8 (2023): 250.
- [41] Johnson, Justin M., and Taghi M. Khoshgoftaar. "Data-centric ai for healthcare fraud detection." *SN Computer Science* 4, no. 4 (2023): 389.
- [42] Sun, Zhenyang, Gangyi An, Yixuan Yang, and Yasong Liu. "Optimized machine learning enabled intrusion detection 2 system for internet of medical things." *Franklin Open* 6 (2024): 100056.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

- [43] Adeniyi, Emmanuel Abidemi, Roseline Oluwaseun Ogundokun, and Joseph Bamidele Awotunde. "IoMT-based wearable body sensors network healthcare monitoring system." *IoT in healthcare and ambient assisted living* (2021): 103-121.
- [44] Rayan, Rehab A., Christos Tsagkaris, and Imran Zafar. "IoT for better mobile health applications." In *A Fusion of Artificial Intelligence and Internet of Things for Emerging Cyber Systems*, pp. 1-13. Cham: Springer International Publishing, 2021.
- [45] Ghubaish, Ali, Tara Salman, Maede Zolanvari, Devrim Unal, Abdulla Al-Ali, and Raj Jain. "Recent advances in the internet-of-medical-things (IoMT) systems security." *IEEE Internet of Things Journal* 8, no. 11 (2020): 8707-8718.
- [46] Gummadi, Anna Namrita, Jerry C. Napier, and Mustafa Abdallah. "XAI-IoT: an explainable AI framework for enhancing anomaly detection in IoT systems." *IEEE Access* 12 (2024): 71024-71054.
- [47] Chandola, Varun, Arindam Banerjee, and Vipin Kumar. "Anomaly detection: A survey." *ACM computing surveys (CSUR)* 41, no. 3 (2009): 1-58.
- [48] Ukil, Arijit, Soma Bandyopadhyay, Chetanya Puri, and Arpan Pal. "IoT healthcare analytics: The importance of anomaly detection." In *2016 IEEE 30th international conference on advanced information networking and applications (AINA)*, pp. 994-997. IEEE,
- [49] Sunny, Jithin S., C. Pawan K. Patro, Khushi Karnani, Sandeep C. Pingle, Feng Lin, Misa Anekoji, Lawrence D. Jones, Santosh Kesari, and Shashaanka Ashili. "Anomaly detection framework for wearables data: a perspective review on data concepts, data analysis algorithms and prospects." *Sensors* 22, no. 3 (2022): 756.
- [50] Buiya, Md Rashed, A. N. Laskar, Md Rafiqul Islam, S. K. S. Sawalmeh, M. S. R. C. Roy, R. E. R. S. Roy, and Md Sumsuzoha. "Detecting IoT cyberattacks: advanced machine learning models for enhanced security in network traffic." *Journal of Computer Science and Technology Studies* 6, no. 4 (2024): 142-152.
- [51] Guo, Hongtai, Zhangbing Zhou, Deng Zhao, and Walid Gaaloul. "EGNN: Energy-efficient anomaly detection for IoT multivariate time series data using graph neural network." *Future Generation Computer Systems* 151 (2024): 45-56.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

- [52] Hernandez-Jaimes, Mireya Lucia, Alfonso Martinez-Cruz, and Kelsey Alejandra Ramírez-Gutiérrez. "A Machine Learning approach for anomaly detection on the Internet of Things based on Locality-Sensitive Hashing." *Integration* 96 (2024): 102159.
- [53] Saba, Tanzila, Amjad Rehman, Tariq Sadad, Hoshang Kolivand, and Saeed Ali Bahaj. "Anomaly-based intrusion detection system for IoT networks through deep learning model." *Computers and Electrical Engineering* 99 (2022): 107810.
- [54] C. Liu, J. Zhao, Z. Song and Y. Dong, "Anomalous Traffic Detection Method for Power Internet of Things Based on Graph Neural Networks," *2023 7th International Conference on Electrical, Mechanical and Computer Engineering (ICEMCE)*, Xi'an, China, 2023, pp. 83-86, doi: 10.1109/ICEMCE60359.2023.10490660.
- [55] Caville, Evan, Wai Weng Lo, Siamak Layeghy, and Marius Portmann. "Anomal-E: A self-supervised network intrusion detection system based on graph neural networks." *Knowledge-based systems* 258 (2022): 110030.
- [56] Balakrishna, Sivadi, M. Thirumaran, and Vijender Kumar Solanki. "IoT sensor data integration in healthcare using semantics and machine learning approaches." *A handbook of internet of things in biomedical and cyber physical system* (2020): 275-300.
- [57] Ali, Farman, Shaker El-Sappagh, SM Riazul Islam, Daehan Kwak, Amjad Ali, Muhammad Imran, and Kyung-Sup Kwak. "A smart healthcare monitoring system for heart disease prediction based on ensemble deep learning and feature fusion." *Information Fusion* 63 (2020): 208-222.
- [58] Bhavsar, Mansi, Kaushik Roy, John Kelly, and Odeyomi Olusola. "Anomaly-based intrusion detection system for IoT application." *Discover Internet of things* 3, no. 1 (2023): 5.
- [59] Najim, Ali Hamza, Kareem Ali Malalah Al-sharhanee, Istabraq M. Al-Joboury, Dimitris Kanellopoulos, Varun Kumar Sharma, Mustafa Yahya Hassan, Walid Issa, Fatima Hashim Abbas, and Ali Hashim Abbas. "An IoT healthcare system with deep

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

learning functionality for patient monitoring." *International Journal of Communication Systems* 38, no. 4 (2025): e6020.

[60] Yang, Geng, Li Xie, Matti Mäntysalo, Xiaolin Zhou, Zhibo Pang, Li Da Xu, Sharon Kao-Walter, Qiang Chen, and Li-Rong Zheng. "A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box." *IEEE transactions on industrial informatics* 10, no. 4 (2014): 2180-2191.

[61] Ali, Zulfiqar, M. Shamim Hossain, Ghulam Muhammad, and Arun Kumar Sangaiah. "An intelligent healthcare system for detection and classification to discriminate vocal fold disorders." *Future Generation Computer Systems* 85 (2018): 19-28.

[62] Qi, Ke. "Advancing hospital healthcare: achieving IoT-based secure health monitoring through multilayer machine learning." *Journal of Big Data* 12, no. 1 (2025): 1.

[63] Sworna, Nabila Sabrin, AKM Muzahidul Islam, Swakkhar Shatabda, and Salekul Islam. "Towards development of IoT-ML driven healthcare systems: A survey." *Journal of Network and Computer Applications* 196 (2021): 103244

[64] Yıldırım, Emre, Murtaza Cicioğlu, and Ali Çalhan. "Fog-cloud architecture-driven Internet of Medical Things framework for healthcare monitoring." *Medical & Biological Engineering & Computing* 61, no. 5 (2023): 1133-1147.

[65] Hathaliya, Jigna J., and Sudeep Tanwar. "An exhaustive survey on security and privacy issues in Healthcare 4.0." *Computer Communications* 153 (2020): 311-335.

[66] McMurray, Samuel, and Ali Hassan Sodhro. "A study on ML-based software defect detection for security traceability in smart healthcare applications." *Sensors* 23, no. 7 (2023): 3470.

[67] Owen, Anthony, and Emma Oye. "Deep Learning-Powered Anomaly Detection for DODAG Control Message Flooding in IoT Networks." (2025).

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

- [68] Zhang, Hanqing, Xuzhong Jia, and Chen Chen. "Deep Learning-Based Real-Time Data Quality Assessment and Anomaly Detection for Large-Scale Distributed Data Streams." (2025).
- [69] Zhu, Guoxiong, Yang Hu, Xiaoning Zhang, Jiyu Chen, and Jizhen Liu. "Applying deep learning and automated machine learning for enhanced state monitoring and health assessment of high-pressure heater in thermal power units." *Engineering Applications of Artificial Intelligence* 141 (2025): 109805.
- [70] Rana, Naresh, Tanishk Thakur, and Shruti Jain. "Smart Seizure Detection System: Machine Learning Based Model in Healthcare IoT." *Current Aging Science* 18, no. 1 (2025): 29-38.
- [71] Atashgahi, Zahra, Mohammadreza Jafaei, Ehsan Nazerfard, and Alireza Nadali. "Anomaly Detection using ConvLSTM Autoencoder in Smart Home Environments."
- [72] Kishor Kumar Reddy, C., Vijaya Sindhoori Kaza, R. Madana Mohana, Mohammed Alhameed, Fathe Jeribi, Shadab Alam, and Mohammed Shuaib. "Detecting anomalies in smart wearables for hypertension: a deep learning mechanism." *Frontiers in Public Health* 12 (2025): 1426168.
- [73] Ntayagabiri, Jean Pierre, Youssef Bentaleb, Jeremie Ndikumagenge, and Hind El Makhtoum. "OMIC: A Bagging-Based Ensemble Learning Framework for Large-Scale IoT Intrusion Detection." *Journal of Future Artificial Intelligence and Technologies* 1, no. 4 (2025): 401-416.
- [74] Wali, Syed, Yasir Ali Farrukh, and Irfan Khan. "Explainable AI and random forest based reliable intrusion detection system." *Computers & Security* (2025): 104542.
- [75] Cai, Saihua, Yingwei Zhao, Jiaao Lyu, Shengran Wang, Yikai Hu, Mengya Cheng, and Guofeng Zhang. "DDP-DAR: Network intrusion detection based on denoising diffusion probabilistic model and dual-attention residual network." *Neural Networks* 184 (2025): 107064.
- [76] Gad, Ibrahim. "TOCA-IoT: Threshold Optimization and Causal Analysis for IoT Network Anomaly Detection Based on Explainable Random Forest." *Algorithms* 18, no. 2 (2025): 117.

ARTIFICIAL NEURAL NETWORK MODEL FOR CLASSIFICATION OF IOT DEVICE STATES IN MEDICAL INDUSTRY

[77] Saheed, Yakub Kayode, and Sanjay Misra. "CPS-IoT-PPDNN: A new explainable privacy preserving DNN for resilient anomaly detection in Cyber-Physical Systems-enabled IoT networks." *Chaos, Solitons & Fractals* 191 (2025): 115939.

[78] Tang, Lun, Ruiyu Wei, Bingsen Xia, Yuanchun Tang, Weili Wang, Qiong Huang, and Qianbin Chen. "Online Anomaly Detection in Industrial IoT Networks Using a Supervised Contrastive Learning-Based Spatiotemporal Variational Autoencoder." *IEEE Internet of Things Journal* (2025).

[79] Qian, Cheng, Wenzhong Tang, and Yanyang Wang. "RGAnomaly: Data reconstruction-based generative adversarial networks for multivariate time series anomaly detection in the Internet of Things." *Future Generation Computer Systems* (2025): 107751.

[80] Deivakani, M. "Anomaly Detection in IoT Network Traffic Using Bidirectional 3D Quasi-Recurrent Neural Network Optimize With Coati Optimization Algorithm." *Transactions on Emerging Telecommunications Technologies* 36, no. 1 (2025): e70026.