Anusandhanvallari
Vol 2023, No.1
April 2023
ISSN 2229-3388

Smart ICU Security Framework Using IoT and Deep Learning-Based Anomaly Detection

[1]Purude Vaishali Narayanrao, [2]P. Manasa, [3]K Raghavendar, [4]Swapna Siddamsetti, [5]Maragoni Mahendar

[1]Assistant Professor, Department of Computer Science and Engineering, Neil Gogte Institute of Technology. Hyderabad, Telangana.

vaishupurude@gmail.com

[2]Assistant Professor, Department of Computer Science and Engineering, Neil Gogte Institute of Technology

reddymanasa24@gmail.com

[3]Assistant Professor, Department of Computer Science and Engineering, TKR college of Engineering and Technology, Meerpet, saroornagar, Rangareddy 500097

Raghavendark20@gmail.com

[4]Assistant Professor Department of Computer Science and Engineering, Neil Gogte Institute of Technology

swapnangit2021@gmail.com

[5]Assistant Professor, Department of Computer Science and Engineering, Neil Gogte Institute of Technology ,Hyderabad, Telangana.

m.mahender527@gmail.com

Abstract: The rapid growth of Internet of Things (IoT) technologies in healthcare has improved patient monitoring and automated medical services, especially in Smart Intensive Care Units (ICUs). However, the increasing number of connected medical devices also exposes healthcare systems to cyber threats and security vulnerabilities. This study proposes an IoT-enabled Smart ICU framework for real-time anomaly detection using advanced machine learning and deep neural network techniques. The BoT-IoT dataset is utilized to train and evaluate the proposed system. Data preprocessing methods such as feature selection, label encoding, SMOTE-based class balancing, and feature standardization are applied to improve model performance. Several machine learning algorithms, including K-Nearest Neighbors (KNN), Random Forest, and XGBoost, are implemented along with deep learning models such as Feedforward Neural Network (FFNN), Deep Neural Network (DNN), Convolutional Neural Network (CNN), and CNN-BiLSTM. In addition, ensemble learning approaches like Voting and Stacking classifiers are used to enhance prediction accuracy and robustness. Experimental results show that the Stacking Classifier achieves the best performance with 99.99% accuracy. Explainable AI techniques such as LIME and SHAP are incorporated for model interpretability. A Flask-based web application is also developed for real-time monitoring and prediction in Smart ICU environments.

Keywords— IoT security, Smart ICU, anomaly detection, deep neural networks, ensemble learning, BoT-IoT dataset, explainable AI, Flask deployment.

INTRODUCTION

The rapid evolution of Internet of Things (IoT) technologies has reshaped modern healthcare infrastructures, particularly within Smart Intensive Care Units (ICUs), where interconnected medical devices continuously collect, transmit, and analyze patient data in real time. These intelligent systems enhance clinical efficiency, enable continuous monitoring, and support proactive medical interventions [1]. AI-powered monitoring frameworks further strengthen patient care by identifying abnormal physiological patterns and supporting early diagnosis in

critical environments [2]. The integration of deep learning with IoT-based healthcare platforms has accelerated the transformation toward data-driven and automated clinical ecosystems [3]. Advanced real-time monitoring solutions in ICUs leverage networked sensors and intelligent analytics to improve patient safety and operational responsiveness [4]. Despite these advancements, the growing dependence on interconnected devices introduces significant cybersecurity vulnerabilities. IoT-enabled healthcare networks generate massive volumes of heterogeneous traffic, making them attractive targets for cyberattacks and intrusion attempts [5]. Edge-based anomaly detection solutions have demonstrated potential in improving reliability and early threat identification within medical IoT systems [6]. Research efforts also emphasize privacy-preserving and intelligent anomaly detection mechanisms to address security concerns in wireless healthcare environments [7]. Hybrid deep learning architectures have been explored to enhance detection accuracy and strengthen resilience against evolving attack patterns in IoT healthcare ecosystems [8].

The convergence of precision healthcare, deep learning, and IoT technologies highlights the necessity for secure, intelligent monitoring frameworks capable of handling complex and high-dimensional network data [9]. Secure and adaptive healthcare monitoring frameworks have demonstrated the importance of combining machine learning techniques with structured intrusion detection mechanisms to protect sensitive patient information and maintain operational continuity [10]. The objective is to design an IoT-enabled Smart ICU security framework capable of detecting anomalous network activities in real time using advanced machine learning and deep learning models. The system aims to enhance detection accuracy, ensure interpretability of predictions, and support secure, reliable, and transparent monitoring within critical healthcare infrastructures while safeguarding patient data and ensuring uninterrupted ICU operations.

RELATED WORK

Qi proposed a multilayer machine learning framework to strengthen IoT-based secure health monitoring within hospital environments, emphasizing layered classification strategies to enhance detection reliability and system robustness [11]. The study highlighted how structured learning pipelines can improve secure data transmission and continuous monitoring performance in interconnected medical infrastructures. Dhanalakshmi and colleagues introduced a real-time monitoring mechanism that tracks patient movement and restraint usage using IoT sensors integrated with deep learning models [12]. Their approach demonstrated how intelligent analytics can support healthcare supervision by identifying abnormal behavioral patterns, thereby improving patient safety and clinical oversight in dynamic hospital settings. Vallabhuni and Debasis developed a hybrid deep learning framework for IoT-based health monitoring that focuses on physiological event extraction from continuous sensor streams [13]. Their work emphasized the importance of combining multiple neural architectures to capture complex biomedical signal characteristics, enabling more accurate anomaly identification in connected healthcare systems. Vithyalakshmi and co-authors presented a wearable IoT-based monitoring system equipped with AI-driven alert mechanisms for real-time patient anomaly detection [14]. Their system leveraged sensor fusion and intelligent classification techniques to provide timely notifications to caregivers, highlighting the growing role of wearable technologies in proactive healthcare management.

Alsaeed and Nadeem explored AI-enabled Internet of Medical Things architectures designed to transform healthcare delivery in smart hospitals [15]. Their contribution underscored the integration of intelligent analytics with interconnected medical devices to support automation, predictive diagnostics, and enhanced decision-making capabilities across distributed healthcare networks. Nafis and collaborators proposed a hybrid deep learning architecture for real-time IV infusion anomaly detection using IoT sensors [16]. Their design focused on cost-effective deployment while maintaining high detection accuracy, demonstrating the practical feasibility of embedding intelligent anomaly detection directly into clinical monitoring equipment. Desai, Rumale, and Asadinia introduced the FAITH framework for fault anomaly identification in healthcare IoT systems using machine learning techniques [17]. Their approach emphasized trustworthy detection mechanisms capable of identifying both

operational faults and malicious anomalies, thereby strengthening reliability and resilience in connected healthcare infrastructures. Alserhani developed a cyber-physical system-based intrusion detection model for medical IoT environments, incorporating adaptive security mechanisms to respond dynamically to emerging threats [18]. The study highlighted the importance of real-time intrusion detection and adaptive response strategies to mitigate risks in highly sensitive clinical networks.

Desai and colleagues further proposed the SHIELD framework, which integrates efficient machine learning models for securing healthcare IoT ecosystems against anomaly-based attacks [19]. Their work demonstrated the effectiveness of optimized classification techniques in detecting irregular network behavior while maintaining computational efficiency in resource-constrained environments. Mishra and co-authors introduced an IoT-based health monitoring system tailored for elderly patient care, integrating machine learning algorithms for predictive health assessment [20]. Their research emphasized continuous monitoring, early risk detection, and intelligent alert generation to improve healthcare quality for vulnerable populations.

MATERIALS AND METHODS

The proposed system presents an IoT-enabled Smart ICU security framework designed for real-time anomaly detection in healthcare network environments. It incorporates structured data ingestion, preprocessing, feature selection, label encoding, class balancing using SMOTE, and feature standardization to ensure high-quality inputs for classification. Baseline machine learning models including KNN, Random Forest, and XGBoost are implemented to establish reliable detection performance. Advanced deep learning architectures such as Feedforward Neural Network (FFNN), Deep Neural Network (DNN), Convolutional Neural Network (CNN), and CNN combined with LSTM are utilized to capture complex spatial and temporal attack patterns in IoT traffic, inspired by intelligent healthcare monitoring frameworks [21].

To improve robustness and generalization, ensemble techniques including Voting Classifier and Stacking Classifier are integrated to combine strengths of diverse models, enhancing predictive stability in dynamic IoT ecosystems [22]. Explainable Artificial Intelligence methods, specifically LIME and SHAP, are incorporated to provide transparent feature-level interpretation of predictions. For deployment, a Flask-based web application enables secure authentication, structured input submission, real-time prediction, and visualization of attack categories, supporting scalable and intelligent healthcare security management [23].

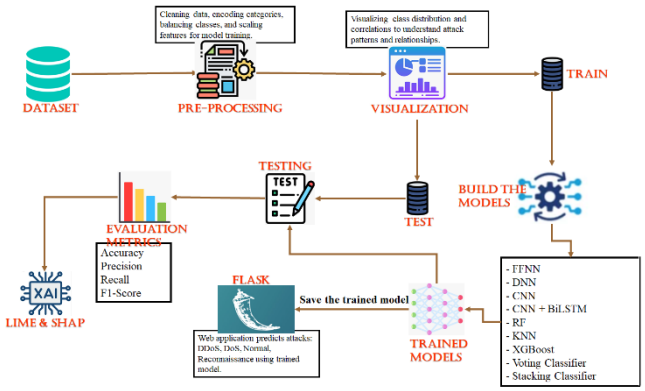

Fig.1 System Architecture

Fig. 1 illustrates a machine learning pipeline for cyberattack prediction. The process begins with raw data undergoing pre-processing—including cleaning and scaling—followed by visualization to identify attack patterns. After training various models like FFNN and Random Forest, the system evaluates performance via metrics like

F1-score and utilizes XAI (LIME/SHAP) for interpretability. Finally, the trained model is deployed in a Flask web application.

A) Dataset Collection:

The dataset collection process utilizes the BoT-IoT dataset, which contains comprehensive network traffic records designed for cybersecurity research and intrusion detection analysis. As illustrated in Fig. 2, the dataset represents a structured snapshot of network flow information comprising multiple traffic attributes such as protocol type (TCP, UDP, ARP), source and destination IP addresses, port numbers, packet counts, byte statistics, and flow-based metrics. Each record includes labeled information specifying attack status, category, and subcategory, enabling supervised learning for anomaly detection. For this study, specific dataset files including data_1.csv, data_16.csv, and data_53.csv are selected to ensure diverse traffic representation. These files are loaded individually and concatenated into a single unified DataFrame to create a consolidated dataset for analysis. This integrated dataset forms the foundation for preprocessing, feature engineering, and model training, supporting the development of an effective intrusion detection framework for Smart ICU network environments.

	pkSeqID	stime	flgs	proto	saddr	sport	daddr	dport	pkts	bytes	...	spkts	dpkts	sbytes	dbytes	rate	srate	drate	attack	category	subcategory
0	1	1.526344e+09	e	arp	192.168.100.1	NaN	192.168.100.3	NaN	4	240	...	2	2	120	120	0.002508	0.000836	0.000836	0	Normal	Normal
1	2	1.526344e+09	e	tcp	192.168.100.7	139	192.168.100.4	36390	10	680	...	5	5	350	330	0.006190	0.002751	0.002751	0	Normal	Normal
2	3	1.526344e+09	e	udp	192.168.100.149	51838	27.124.125.250	123	2	180	...	1	1	90	90	20.590960	0.000000	0.000000	0	Normal	Normal
3	4	1.526344e+09	e	arp	192.168.100.4	NaN	192.168.100.7	NaN	10	510	...	5	5	210	300	0.006189	0.002751	0.002751	0	Normal	Normal
4	5	1.526344e+09	e	udp	192.168.100.27	58999	192.168.100.1	53	4	630	...	2	2	174	456	0.005264	0.001755	0.001755	0	Normal	Normal

5 rows × 35 columns

Fig.2 Dataset

B) Pre-Processing:

Pre-processing is a crucial stage that transforms raw network traffic data into a structured and reliable format suitable for analysis. Since IoT-generated datasets often contain redundant attributes, missing values, and imbalanced class distributions, systematic cleaning and transformation are essential. This stage improves data consistency, enhances learning efficiency, and ensures meaningful pattern extraction for anomaly detection.

Pre-processing: The pre-processing phase begins with removing unwanted and irrelevant columns that do not contribute to anomaly detection, such as identifiers or redundant metadata fields. Eliminating these attributes reduces noise, minimizes computational complexity, and improves overall data quality. The dataset is then examined for missing or inconsistent values. Any incomplete records are either removed or appropriately imputed to maintain data integrity while preventing bias in the learning process.

Categorical features such as protocol type and service information are transformed into numerical representations using label encoding. This conversion ensures compatibility with computational models while preserving categorical distinctions. Since network intrusion datasets commonly exhibit class imbalance, especially between normal and attack traffic, Synthetic Minority Over-sampling Technique (SMOTE) is applied to balance the dataset. This step prevents bias toward majority classes and improves representation of minority attack categories.

Finally, numeric features such as packet counts, byte rates, and flow statistics are standardized. Standardization scales features to a uniform range, preventing dominance of high-magnitude attributes and enabling stable learning behavior. These comprehensive preprocessing steps ensure the dataset is clean, balanced, and structured for effective anomaly detection in Smart ICU environments.

Data Visualization: Data visualization is performed to understand traffic distribution patterns and relationships among features before model development. The first visualization focuses on attack category class distribution. This analysis illustrates the proportion of normal and different attack categories present in the dataset. Understanding class distribution is essential to identify imbalance issues and evaluate the diversity of intrusion types. A clear visualization helps reveal whether certain attacks dominate the dataset or if normal traffic significantly outweighs malicious activity. Such insights guide decisions related to balancing strategies and dataset preparation.

The second visualization involves generating a correlation matrix to examine relationships between numerical features. The correlation matrix highlights the strength and direction of associations among traffic attributes such as packet counts, byte rates, and flow duration. Strong correlations may indicate redundancy, while weak correlations can reveal independent informative features. Visual inspection of correlation patterns supports feature understanding and helps identify multicollinearity issues. By analyzing these visual representations, meaningful insights are derived regarding traffic behavior, feature interdependence, and dataset structure, thereby supporting more informed data preparation and system design decisions.

Train and Test Splitting: After preprocessing and visualization, the dataset is divided into training and testing subsets to ensure objective evaluation. The splitting process separates the dataset into two distinct portions, where the training set is used to learn traffic patterns and the testing set is reserved for performance validation. This separation prevents data leakage and ensures that evaluation reflects real-world generalization capability.

Typically, a larger proportion of the dataset is allocated for training to enable comprehensive pattern learning, while a smaller portion is reserved for testing. The split is performed in a stratified manner to maintain consistent class distribution across both subsets. Stratification ensures that each attack category is proportionally represented in both training and testing data, preventing skewed evaluation results.

The training subset supports internal pattern discovery and behavioral learning from diverse IoT traffic characteristics. The testing subset simulates unseen network traffic conditions, allowing assessment of detection capability in realistic deployment scenarios. This structured splitting strategy ensures fairness, reliability, and robustness in evaluating anomaly detection performance within Smart ICU network environments.

C) Algorithms:

K-Nearest Neighbors: K-Nearest Neighbors is a supervised learning algorithm that classifies instances based on distance similarity measures. It identifies the k closest data points in feature space and assigns the majority class among neighbors to the new instance. Distance metrics such as Euclidean distance are commonly applied. In IoT-based anomaly detection, it analyzes network traffic patterns and compares them with stored labeled instances to determine whether behavior is normal or malicious. It is simple, non-parametric, and effective for structured numerical data, especially after feature scaling. The model adapts well to multi-class classification tasks and serves as a strong baseline for comparing advanced intelligent detection techniques.

Random Forest: Random Forest is an ensemble learning technique that constructs multiple decision trees during training and combines their outputs for classification. Each tree is trained on random subsets of data and features, increasing diversity and reducing overfitting. The final prediction is determined through majority voting among individual trees. In IoT network monitoring, it evaluates traffic features and detects anomalies by capturing nonlinear relationships between attributes. It handles high-dimensional data efficiently and is robust to noise and missing values. Feature importance scores derived from the model help identify influential network parameters, making it suitable for complex intrusion detection scenarios in Smart ICU environments.

XGBoost: XGBoost is an optimized gradient boosting algorithm that builds decision trees sequentially, where each new tree corrects errors made by previous trees. It incorporates regularization techniques to prevent

overfitting and improve generalization. The model handles sparse data efficiently and supports parallel computation for faster training. In IoT anomaly detection, it learns complex feature interactions within network traffic data to distinguish between normal and attack patterns. Its boosting mechanism enhances predictive strength by minimizing loss iteratively. Due to scalability and high computational efficiency, it performs effectively in large-scale cybersecurity datasets with diverse attack categories.

Feedforward Neural Network: A Feedforward Neural Network consists of multiple fully connected layers where information flows in one direction from input to output. Each neuron applies weighted transformations followed by nonlinear activation functions. The network learns feature representations through backpropagation and gradient descent optimization. In IoT-based intrusion detection, it processes standardized traffic features to identify hidden patterns associated with anomalies. By stacking dense layers, the network captures complex nonlinear relationships among attributes. It supports multi-class classification and adapts well to high-dimensional data. Its layered structure enables automated feature learning, reducing reliance on manual feature engineering for detecting suspicious activity.

Deep Neural Network: A Deep Neural Network extends the feedforward structure by incorporating multiple hidden layers, enabling hierarchical feature extraction. Each layer transforms input representations into higher-level abstractions through nonlinear activations. Training is achieved using backpropagation with optimization algorithms that adjust weights iteratively. In Smart ICU network security, the deep architecture captures intricate dependencies within IoT traffic data, improving representation of subtle attack signatures. The depth of the network allows modeling of complex interactions that shallow models may overlook. It is particularly suitable for large datasets where deep layered representations enhance discrimination between normal and malicious communication patterns.

Convolutional Neural Network: A Convolutional Neural Network applies convolution operations to automatically extract local feature patterns from structured input data. Convolutional layers use filters to capture spatial relationships, followed by pooling layers for dimensionality reduction. Although commonly used in image processing, CNNs can be adapted for network traffic analysis by reshaping feature vectors into structured formats. In IoT anomaly detection, it identifies localized correlations among traffic attributes and learns hierarchical feature maps. Weight sharing reduces the number of parameters and improves computational efficiency. This structure enhances pattern recognition capability for detecting sophisticated intrusion behaviors within multidimensional network data.

CNN with BiLSTM: CNN with BiLSTM combines convolutional layers for spatial feature extraction and Bidirectional Long Short-Term Memory layers for sequential pattern learning. The convolution component captures local correlations among features, while the BiLSTM processes data in forward and backward temporal directions to learn contextual dependencies. This hybrid structure is effective when network traffic exhibits sequential characteristics over time. In IoT environments, it models both feature interactions and temporal behavior of communication flows. The bidirectional mechanism strengthens contextual understanding, enabling detection of evolving attack patterns. The integration of spatial and temporal learning improves representation quality for dynamic intrusion detection scenarios.

Voting Classifier: Voting Classifier is an ensemble approach that aggregates predictions from multiple individual models to produce a final decision. It operates using hard voting, where majority class determines output, or soft voting, where predicted probabilities are averaged. By combining diverse classifiers, it reduces variance and enhances stability. In IoT anomaly detection, it integrates strengths of different machine learning and deep learning models to improve robustness against varied attack patterns. This collective decision-making strategy mitigates weaknesses of individual models and increases reliability in critical healthcare network monitoring systems requiring consistent and accurate classification.

Anusandhanvallari
Vol 2023, No.1
April 2023
ISSN 2229-3388

Stacking Classifier: Stacking Classifier is an ensemble technique that combines multiple base models and employs a meta-learner to generate final predictions. Base models are trained on the original dataset, and their outputs serve as inputs to the higher-level learner. This layered learning strategy captures complementary strengths of different algorithms. In Smart ICU network security, stacking enables integration of heterogeneous classifiers to model complex traffic patterns effectively. The meta-learner optimizes decision boundaries based on combined predictions, enhancing generalization capability. This hierarchical ensemble mechanism strengthens detection performance in multi-class IoT intrusion classification tasks.

I. Experimental Results

Accuracy: The accuracy of a test is its ability to differentiate the patient and healthy cases correctly. To estimate the accuracy of a test, we should calculate the proportion of true positive and true negative in all evaluated cases. Mathematically, this can be stated as:

$$Accuracy = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{FP} + \mathrm{TN} + \mathrm{FN}} (1)$$

Precision: Precision evaluates the fraction of correctly classified instances or samples among the ones classified as positives. Thus, the formula to calculate the precision is given by:

$$Precision = \frac{\text{True Positive}}{\text{True Positive } + \text{False Positive}} (2)$$

Recall: Recall is a metric in machine learning that measures the ability of a model to identify all relevant instances of a particular class. It is the ratio of correctly predicted positive observations to the total actual positives, providing insights into a model's completeness in capturing instances of a given class.

$$Recall = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} (3)$$

F1-Score: F1 score is a machine learning evaluation metric that measures a model's accuracy. It combines the precision and recall scores of a model. The accuracy metric computes how many times a model made a correct prediction across the entire dataset.

$$F1\ Score = 2 * \frac{Recall\ \mathrm{X}\ Precision}{Recall + Precision} * 100 (1)$$

Table.1 Performance Evaluation Table

Model	Accuracy	Precision	Recall	F1 score
FFNN	0.9890	0.9893	0.9890	0.9890
DNN	0.9890	0.9894	0.9890	0.9890
CNN	0.9854	0.9859	0.9854	0.9854
CNN+BiLSTM	0.9862	0.9866	0.9862	0.9862
Random Forest	0.9971	0.9971	0.9971	0.9971
KNN	0.9995	0.9995	0.9995	0.9995
XGBoost	0.9972	0.9973	0.9972	0.9972
Voting Classifier	0.9998	0.9999	0.9998	0.9998
Stacking Classifier	**0.9999**	**0.9999**	**0.9999**	**0.9999**

Table.1 presents comparative performance evaluation of baseline, deep learning, and ensemble models demonstrating superior accuracy and classification effectiveness.

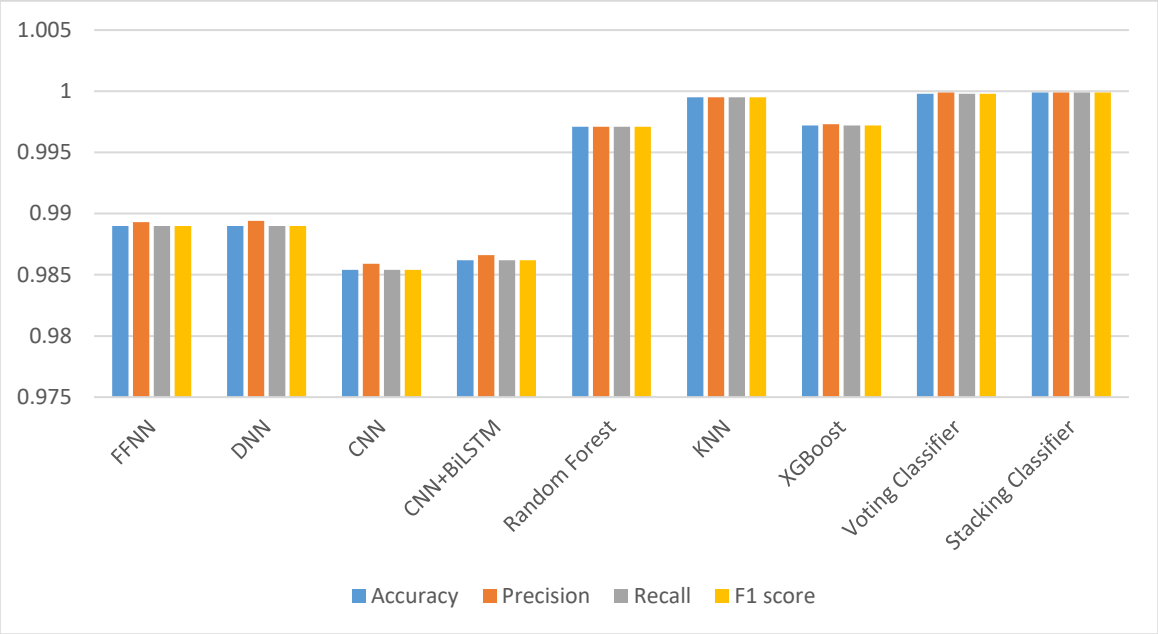

Fig.3 Comparison Graph

Fig. 3 compares various machine learning models, showing that ensemble methods like Stacking and Voting achieve the highest classification performance.

II. Conclusion

The developed IoT-enabled Smart ICU framework demonstrates highly reliable real-time anomaly detection capability for securing critical healthcare infrastructures. Comprehensive preprocessing, including feature engineering, class balancing using SMOTE, and normalization, ensured robust model training on the BoT-IoT dataset. Multiple machine learning and deep learning models were evaluated to identify the most effective architecture for intrusion detection in IoT-based clinical environments. Among all evaluated techniques, the Stacking Classifier achieved the highest performance with 99.99% accuracy, precision, recall, and F1-score, followed closely by the Voting Classifier with 99.98% accuracy, indicating exceptional detection capability with minimal false positives and false negatives. The integration of Explainable Artificial Intelligence techniques, specifically LIME and SHAP, provided meaningful insights into feature contributions and enhanced transparency in model predictions. This interpretability is critical in healthcare settings, where trust and accountability are essential for deployment. Furthermore, the implementation of a Flask-based web application enabled real-time prediction through an interactive user interface, supporting practical usability in Smart ICU environments. The overall outcome establishes a secure, interpretable, and high-performance anomaly detection framework suitable for safeguarding IoT-enabled medical systems against evolving cyber threats.

Future enhancements can focus on deploying the trained ensemble model within a real-time streaming environment using live IoT sensor data from Smart ICU devices. Integration with edge computing architectures can significantly reduce latency and enhance response time for mission-critical healthcare operations. Exploration of transformer-based deep learning architectures may further improve detection capability against sophisticated and zero-day cyber threats. Incorporating federated learning can support privacy-preserving distributed training across multiple healthcare institutions without centralized data sharing. Expanding interpretability mechanisms with advanced explanation frameworks can enhance transparency in security decisions. Additionally, large-scale

validation using real hospital network traffic and adaptive self-learning models can improve scalability, robustness, and resilience against continuously evolving cyberattacks in IoT-enabled healthcare ecosystems.

REFERENCES

[1] Ranjan, R., Raj, A., Shreyash, S., Bhardwaj, D., Verma, D., & Gupta, S. (2025, September). Deep Learning based Early Detection of Cardiovascular Anomalies in IoT-Enabled Smart Hospitals. In 2025 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp. 1-7). IEEE.

[2] Punith, M., Nirmala, M. B., & Swathi, P. G. (2025, October). AI-Powered Real-Time Patient Monitoring System with Hybrid Health Anomaly Detection. In 2025 International Conference on Communication, Computer, and Information Technology (IC3IT) (pp. 01-13). IEEE.

[3] Alharbe, N., & Almalki, M. (2025). IoT-enabled healthcare transformation leveraging deep learning for advanced patient monitoring and diagnosis. Multimedia Tools and Applications, 84(19), 21331-21344.

[4] Bai, Y., Gu, B., & Tang, C. (2025). Enhancing real-time patient monitoring in intensive care units with deep learning and the internet of things. Big Data.

[5] Abdulkhudhur, S. M., Abboud, S. M., Najim, A. H., Kadhim, M. N., & Ahmed, A. A. (2025). A Hybrid Deep Belief Cascade-Neuro Fuzzy Approach for Real-Time Health Anomaly Detection in 5G-Enabled IoT Medical Networks. International Journal of Intelligent Engineering & Systems, 18(5).

[6] Hizem, M., Bousbia, L., Ben Dhiab, Y., Aoueileyine, M. O. E., & Bouallegue, R. (2025). Reliable ECG Anomaly Detection on Edge Devices for Internet of Medical Things Applications. Sensors, 25(8), 2496.

[7] Thenmozhi, P., & Ramathilagam, A. (2025, August). A survey on AI-enabled anomaly detection with privacy preservation in wireless sensor healthcare IoT environment. In 2025 IEEE 6th International Conference in Robotics and Manufacturing Automation (ROMA) (pp. 334-338). IEEE.

[8] Kavitha, M. S., Sreeja, G. G., Karthik, S., & Sabitha, R. (2025). Reforming disease prognosis and treatment prediction for palliative care with hybrid metaheuristic deep neural architectures in IoT healthcare ecosystems. Scientific Reports.

[9] Feng, G., Manimurugan, S., Yi, B., & Feng, Y. (2025). Towards Precision Cardiac Healthcare: Deep Learning and IoT Integration for Real-Time Monitoring and Personalized Diagnosis. IEEE Internet of Things Journal.

[10] Sagar, R., Kumar, N. S., Sastry, A. S., Krishna, N., & Reshma, S. (2025). SHMADF: A Secure and Intelligent Framework for IoT-Enabled Healthcare Monitoring and Attack Detection. Annals of Data Science, 1-38.

[11] Qi, K. (2025). Advancing hospital healthcare: achieving IoT-based secure health monitoring through multilayer machine learning. Journal of Big Data, 12(1), 1.

[12] Dhanalakshmi, S., Jayanthi, L. N., Sangeetha, P., Gowri, J. B., Karthikeyan, S., & Rajmohan, M. (2025, March). Real-Time Monitoring of Patient Movement and Restraint Usage in healthcare Settings with IoT and Deep Learning Model. In 2025 International Conference on Visual Analytics and Data Visualization (ICVADV) (pp. 360-365). IEEE.

[13] Vallabhuni, S., & Debasis, K. (2025). Hybrid deep learning for IoT-based health monitoring with physiological event extraction. Digital Health, 11, 20552076251337848.

[14] Vithyalakshmi, N., Madhu, B. K., Vekariya, V., & Shrivastava, G. (2025, May). Wearable IoT-based Health Monitoring System with AI-Driven Alerts for Real-Time Patient Anomaly Detection. In 2025 3rd International Conference on Data Science and Information System (ICDSIS) (pp. 1-5). IEEE.

[15] Alsaeed, N., & Nadeem, F. (2025). AI-enabled IoMT: transforming healthcare in smart hospitals. In Blockchain and Digital Twin for Smart Hospitals (pp. 459-496). Elsevier.

[16] Nafis, M. B., Paramita, C., & Wright, S. G. (2025). A Hybrid Deep Learning Architecture for Cost-Effective, Real-Time IV Infusion Anomaly Detection using IoT Sensors. Jurnal Teknik Informatika (Jutif), 6(6), 5956-5975.

[17] Desai, M., Rumale, A., & Asadinia, M. (2025, August). FAITH: Fault Anomaly Identification Using Machine Learning for Trusted Healthcare IoT. In International Conference on Software Engineering of Emerging Technology (pp. 167-178). Cham: Springer Nature Switzerland.

[18] Alserhani, F. (2025). Intrusion detection and real-time adaptive security in medical IoT using a cyber-physical system design. Sensors, 25(15), 4720.

[19] Desai, M., Rumale, A., & Asadinia, M. (2025, May). SHIELD: securing healthcare IoT with efficient machine learning techniques for anomaly detection. In 2025 IEEE World AI IoT Congress (AIIoT) (pp. 0521-0528). IEEE.

[20] Mishra, A. K., Yadav, A. K., Singh, J., Singh, P., Diwakar, M., & Tiwari, M. (2025). A Novel Health Monitoring System Utilizing IoT and Machine Learning Techniques for Elderly Patient Care. In Empowering Solutions for Sustainable Future in Science and Technology (pp. 1-8). Cham: Springer Nature Switzerland.

[21] Manjhi, L., & Sinha, A. P. (2025). Real-Time Health Monitoring Using IoT Sensors and Predictive Machine Learning Models. Journal of Computational Analysis & Applications, 34(9).

[22] Son, N. K., Sangaiah, A. K., Chun-Chi, C., Hsu, H., Hsu, C. C., & Chang, C. Y. (2025). AutoKAN: A federated lightweight anomaly detection framework for securing constrained IoT healthcare diabetes monitoring systems. IEEE Transactions on Consumer Electronics.

[23] Wang, X., Yue, X., Tariq, N., & Sajid, A. (2025). Hybrid AI-and Blockchain-Powered Secure Internet Hospital Communication and Anomaly Detection in Smart Cities. Processes, 13(5), 1466.

[24] Lokhande, P. P., & Chinnaiah, K. (2025). Heart Disease Detection and Prognosis Using IoT-Based ECG Sensor Data with Hybrid Deep Learning Architecture and Optimal Resource Allocation. Cybernetics and Systems, 1-51.

[25] Najim, A. H., Al-sharhanee, K. A. M., Al-Joboury, I. M., Kanellopoulos, D., Sharma, V. K., Hassan, M. Y., ... & Abbas, A. H. (2025). An IoT healthcare system with deep learning functionality for patient monitoring. International Journal of Communication Systems, 38(4), e6020.