International Journal of Emerging Research in Engineering and Technology
Pearl Blue Research Group | Volume 7 Issue 2 PP 273-281, 2026
ISSN: 3050-922X | https://doi.org/10.63282/3050-922X.IJERET-V7I2P133

Original Article

Intelligent IoT-Enabled Deep Learning System for Advanced Cybersecurity Anomaly Detection

Vikas Kumar Pandey
Senior Software Engineer, PayPal India Pvt. Ltd. Whitefield, Bangalore, India.

Received On: 16/04/2026 ***Revised On: 15/05/2026*** ***Accepted On: 23/05/2026*** ***Published On: 29/05/2026***

Abstract - *The Internet of Things (IoT) is rapidly increasing attack surface of cyber threats, making the existing security measures insufficient to detect complex and dynamic abnormalities. The article presents a plan for a sophisticated system that uses deep learning (DL) and the internet of things (IoT) to identify cybersecurity irregularities using a CNN-BiLSTM architecture. Convolutional Neural Networks (CNNs) easily extract geographic information, whereas Bidirectional Long Short-Term Memory (BiLSTM) networks detect temporal correlations in network data. After label encoding, normalization, and SMOTE-based data balancing, the proposed model is evaluated on the UNSW-NB15 dataset, thereby increasing its consistency. As shown in experiments, the suggested hybrid model has a higher performance rate as it reaches 99.3% testing accuracy (acc), high precisions (prec), recall (rec), and a low FNR, which is significantly better than the traditional machine learning (ML) and standalone models of DL. The system successfully identifies both known and undiscovered cyber threats, making it ideal for real-time IoT applications. This study promotes the idea of scalable, accurate, and intelligent IDS to safeguard modern IoT networks.*

Keywords - *IoT Security, Cybersecurity, Anomaly Detection, Deep Learning, CNN, BiLSTM, Intrusion Detection System, UNSW-NB15, SMOTE, Network Security.*

1. Introduction

IoT enables smart devices and sensors to connect without direct human intervention, which requires processing in near real-time. With the increasing demand and growth of IoT automated network systems, IoT models are becoming more complex day by day [1][2]. The growing complexity of IoT infrastructures is increasing vulnerabilities in their systems. Cybersecurity is a crucial part of the current IoT environment's information management structure [3][4][5]. In IoT devices, security breaches and anomalies have become increasingly common. IoT raises the possibility of cyberattacks even as it boosts productivity and efficiency through intelligent, remote control. IoT devices use wireless media to broadcast data, making them easier targets for attacks [6][7]. Normal communication attacks are confined to local nodes or a small domain within the local network, whereas attacks in IoT locations may be more severe because the system can span a wider region. Therefore, in order to prevent cybercrime, a secure IoT infrastructure is required. The security measures in place have become vulnerable due to IoT devices' inherent weaknesses [8]. IoT node vulnerabilities create a backdoor via which an attacker can obtain private information from any significant enterprise. Numerous serious flaws in IoT networks also provide a risk [9].

Ransomware, botnet attacks, and DDoS (Distributed Denial of Service) are common cyberattacks that aim to take advantage of IoT networks and degrade their processing power[10]. These devices generate exponentially more data, some of which may include sensitive information. To improve, because hostile attacks on critical infrastructure are increasing, proactive defence technology is required for the security of crucial systems. Commercial security solutions frequently focus primarily on thresholds, signatures, heuristics-driven methods, or data. These methods are effective against known dangers, but they are ineffective against unknown or novel threats. Additionally, these techniques usually need training, subject-matter expertise, and continuous improvements [11][12]. The inability to identify new cyberthreats and the need to have advanced systems.

In order to overcome these constraints, DL and ML approaches have become effective IoT cybersecurity solutions [13]. Widespread applications of these methods include classification, regression, intrusion detection, image analysis, and recommendation systems. Since the ML-based models are capable of identifying patterns in the data, it becomes more accurate to detect both known and unrecognized threats [14][15]. Specifically, DL methods have also shown to hold great potential in the creation of sophisticated intrusion detection systems (IDS) through automatic discovery of complex traits in large volumes of IoT data [16]. Such intelligent systems promote real-time detection of anomalies and cyberattacks, which is extremely useful in the context of the current IoT ecosystems [17][18]. Because of increasing quantity of linked devices and online threats, the creation of highly efficient and smart intrusion detection has gained even greater significance. IDS is crucial in detecting malicious behaviours, network intrusions, and, in general, the security of IoT environments.

1.1. Motivation and Contribution

The increasing number of IoT gadgets in several crucial sectors, such as industrial systems, smart cities, and healthcare, has exposed networks to complex and comprehensive cyber threats. The traditional methods of security are not effective in identifying unknown and dynamic attacks since they are based on known signatures and policies. Besides, the large amount of data, speed, and variability of IoT require smart and dynamic detection systems. That promotes the development of a dependable Anomaly detection method based on DL that can

recognize intricate patterns, imbalanced data, and offer high detection rates. This study was prompted by requirement to have a scalable, automated, and real-time cybersecurity key. The following are paper's primary contributions:

- Proposed a hybrid CNN-BiLSTM DL model of IoT-based cybersecurity anomaly detection.
- Integrated spatial feature extraction (CNN) with temporal sequence learning (BiLSTM) for improved detection performance.
- Applied SMOTE-based data balancing to handle class imbalance and improve minority attack detection.
- Conducted extensive preprocessing, such as normalization and label encoding to train a model efficiently.
- Developed a framework that could be used in real-time and scalable IoT cybersecurity applications.

1.2. Justification And Novelty

The research addresses the severe shortcomings of current IoT cybersecurity solutions by proposing a CNN-BiLSTM hybrid architecture that concurrently records network traffic's temporal and spatial characteristics. The proposed framework as opposed to the traditional models, which concentrate on the accuracy aspect only, concentrates on robustness, generalization, and flexibility towards the changing cyber threats. Deep learning combined with SMOTE also boosts the detection of minority attack classes. It is novel in that it integrates efficient feature extraction and bidirectional temporal learning, leading to an extremely accurate and reliable anomaly detection system in dynamic IoT environments.

1.3. Organization of the Paper

The following is the structure of the paper: The paper is organized as follows: Section II discusses previous research in the field, Section III describes the dataset, data preprocessing, and proposed methodology, Section IV presents the experimental results and a comparison of those results, and Section V concludes the paper by summarizing the main findings and offering suggestions for future research.

2. Literature Review

Recent literature on IoT cybersecurity anomaly detection explores advanced ML and DL models achieving high accuracy, while still lacking lightweight, real-time, and edge-deployable solutions for dynamic environments.

S. Manekar (2026) proposes an effective cybersecurity anomaly detection model of the IoT that is founded on an integration of ANN and LSTM models. It used the IoT-23 dataset, which comprised multiple malware and normal traffic captures, followed by the preprocessing phase of cleaning, normalizing, and feature selection. To improve model performance and data quality, what exploratory data analysis and preprocessing aims to do is choose features and normalize them. With an acc, prec, and F1 of 98.6%, experimental data show that the Hybrid ANN+LSTM model outperforms more conventional ML models like ANN, SVM, and Naive Bayes [19].

M. P. K et al. (2025) proposed system exhibits outstanding performance with 99.21 % detection rate, 99.07% prec, 99.15% rec, 99.18% F1, and it provides an effective way of identifying threats like DDoS, SQL Injection, and Ransomware. In conclusion, Cyber-CapG provides a solid solution for traffic surveillance in IoT/IIoT, providing high detection and prevention of various cyber threats, as well as optimizing the cybersecurity and reliability of industrial networks [20].

S. Aslam, M. M. R. Alshoweky, and M. Saad (2024) present a method for detecting cyberattacks for IIoT applications using the Edge-IIoT set dataset. The proposed detection approach divides cyberattacks in IIoT networks into binary and multiple groups using ML (LR and DT) and DL (recurrent and CNN). With an average acc of 90%, the suggested categorization methods demonstrate the efficacy of the used algorithms [21].

X. Li et al. (2024) to address this problem, MH-DRNN were developed. The system minimizes issues that come with heterogeneous data analysis using the process of feature selection and classification optimization. The optimization strategy decreases the computational demands by selecting features of the sunflower movement-based feature set. Moreover, this system has three MLPs and three recurrent layers to maximize the prediction rate with the highest accuracy (99.2%) [22].

S. Chakraborty et al. (2023) have suggested using a deep neural network as a framework to address issue of identifying novel attacks with a rule-based approach. The CICIDS 2017 dataset and other benchmark results are greatly enhanced by built framework. The experiment's results demonstrate that suggested model strikes a fair compromise between rates of attack detection, FP, and FN. When it comes to new attacks, model's acc is over 99%. The primary issues when the network devices connect automatically IoT are security and privacy. The proposed solution able to handle these issues and eventually determine and classify the different levels of danger [23].

L. Zhao et al. (2022) in order to reduce noise in data, build an S-G (Savitzky-Golay) filter. Furthermore, to identify sensor numerical anomalies in industrial control systems, a GA-ELM model is suggested. The feature dimensions are reduced from 51 to 10 using the GA, and anomalies are identified by classification using the ELM approach. Lastly, classification accuracy is 98.96% utilizing the Secure Water Treatment (SWaT) public dataset. It shows better outcomes from the suggested approach [24].

Table I is my synthesis of the IoT cybersecurity literature, comparing paradigms, data sets, performance, and constraints, and noting the progress in DL solutions and the persistence in knowledge gap in real-time edge deployments.

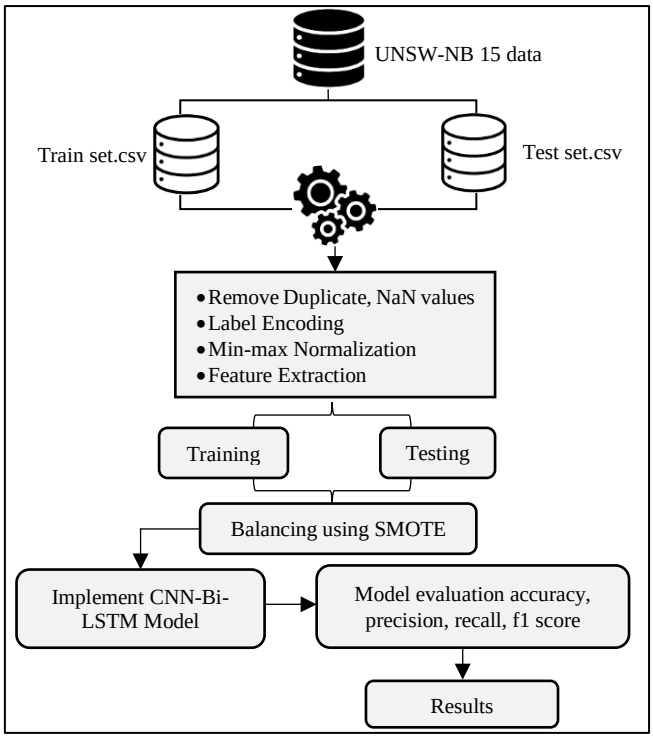

Fig 1: Workflow of the Proposed Deep Learning model for Anomaly Detection in IoT

Table 1: Review of Existing ML and DL Models for IoT IDS

Authors	Approach	Dataset	Application Domain	Performance	Key Contribution	Limitation
S. Manekar (2026)	ANN + LSTM Hybrid Model	IoT-23	IoT malware / anomaly detection	98.6% accuracy	Hybrid ANN-LSTM improves IoT traffic classification	Lacks real-time streaming capability and edge deployment optimization
M. P. K et al. (2025)	Cyber-CapG Deep Learning Model	IoT/IIoT traffic dataset	Cybersecurity anomaly detection	99.21% detection rate	Detects DDoS, SQL Injection, Ransomware effectively	High computational cost, unsuitable for resource-constrained IoT devices
S. Aslam, M. M. R. Alshoweky, and M. Saad (2024)	ML + CNN + RNN Hybrid Classification	Edge-IIoTset dataset	IIoT intrusion detection	~90% accuracy	Multi-class and binary classification of cyber attacks	Lower accuracy and weak long-term dependency modeling
X. Li et al. (2024)	Meta-Heuristic Deep Random Neural Network, (MH-DRNN)	Industrial IoT datasets	Anomaly detection	99.2% accuracy	Feature selection using metaheuristic optimization improves prediction	High complexity and no real-time inference support
S. Chakraborty et al. (2023)	Rule-Based Deep Neural Network	CICIDS2017 dataset	Network intrusion detection	>99% accuracy	Strong detection of novel and unknown attacks	Poor generalization for evolving zero-day attacks
L. Zhao et al. (2022)	GA-ELM + Savitzky-Golay Filtering	SWaT dataset	Industrial control system security	98.96% accuracy	Noise reduction + optimized feature selection	Traditional ML approach, lacks deep learning scalability

Putteti et al. (2025)	ML + DL + Blockchain-based IIoT framework	Industrial IoT environment	Predictive maintenance + security	~95% improvement	Secure data sharing using blockchain in IIoT	Focus more on maintenance than pure cybersecurity anomaly detection

Research gap: The bulk the majority existing solutions have serious limitations, notwithstanding the significant advancement in IoT-enabled cybersecurity anomaly detection techniques brought on by ML and DL techniques. Even though some of the models have potential to be promising in regard to detection accuracy, In an IoT environment with limited resources, they are computationally demanding and cannot be implemented in real time. Additionally, some of them are limited in their efficacy in dynamic attack circumstances as a result of their failure to identify long-term temporal correlations in network data. The generalization to unseen or zero-day attacks is also a problem for traditional and hybrid methods. Moreover, most current systems prioritize accuracy improvements while overlooking lightweight design and edge-based deployment requirements.

2. Research Methodology

The UNSW-NB15 dataset, this is split into test and training sets for methodical examination, is first step in the recommended technique (Fig. 1). Preprocessing of data is conducted to improve quality of data, such as elimination of duplicate and missing (NaN) data, and then the data is label encoded to transform the categorical data into numerical. The characteristics normalized to a common range using min-max normalization, and appropriate feature extraction methods employed to enhance efficiency of model. The processed data is then used for testing and training. In order to overcome issue of class imbalance, SMOTE technique is used to create artificial samples and balance the distribution of classes. Next, temporal and spatial patterns are extracted from the data using a hybrid CNN-BiLSTM model. Finally, model is evaluated using performance metrics, including acc, prec, rec, and F1, and results are analyzed.

This Flowchart may find a detailed explanation of the whole proposed procedure in this section:

2.1. Data Gathering and Analysis

The UNSW-NB15 data set only includes two classifications, "attack" and "normal," which encompass both current usual traffic patterns and attack patterns. It is utilized. The Australian Centre for Cyber Security (ACCS) network-wide laboratory used IXIA PerfectStorm tool35 to construct the first network packet for UNSW-NB15 dataset. It tested 100GB of unmodified traffic by the use of tcpdump. This dataset includes 9 different kinds of attacks. The training set may be found in the file UNSW-NB15 training-set.csv, whereas the testing set has 82,332 items. On display in Fig. 2 is the distribution of both normal/attack data.

Fig. 2 displays the overall distribution of classes in the UNSW-NB15 dataset, which includes an imbalance of records of assaults relative to regular traffic. This skew implies that a dataset is biased towards malicious cases, and they can be biased by the ML models unless mitigated during training.

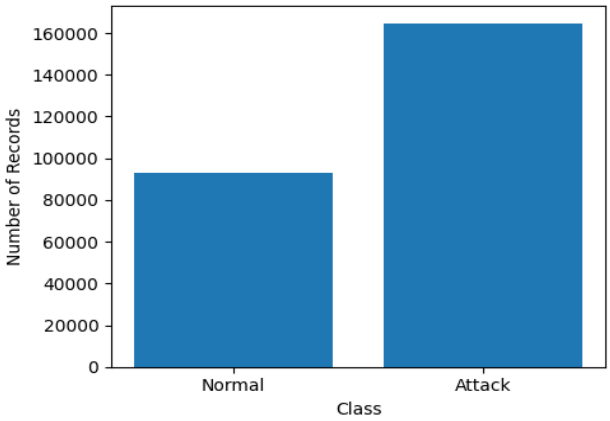

Fig 2: Data Distribution of the Dataset

Fig. 3 shows the distribution of various kinds of attacks in the dataset. It emphasizes how some attack types, such as exploits and generic attacks are more prevalent than others, such as Worms and Shellcode, which have relatively low numbers per class and a highly skewed multi-class distribution.

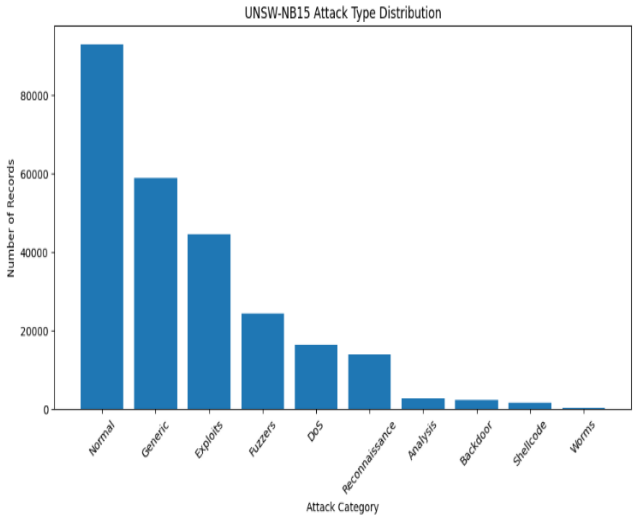

Fig 3: Distribution of Attack Types of the Data

2.2. Data Pre-Processing

The term "data preprocessing" refers to process of cleaning and preparing raw data for efficient analysis and model building. The following are the most significant preprocessing processes that have been used in this study:

- Handle missing value: Determining and dealing with missing data using methods like removal, interpolation, or imputation, based on the kind and quantity of the absent variables.

- Remove Duplicate: The practice of removing redundant data from a dataset that might adversely affect the analysis is known as data deduplication.
- Label Encoding: The dataset includes categorical variables in the form of objects that cannot be directly entered into DL models that need numerical values. To circumvent this, each category is encoded by the use of Label Encoding assigning each category a unique integer. This transformation maintains the consistency of information and compatibility of the model and does not lose the distinction of the classes. As a result, the data is ready for effective processing, and the model is able to identify trends and make accurate predictions.

2.3. Feature Normalization using Min-Max

Scaling techniques play a role in pre-processing domain data in ML, which makes predictive models more impactful and solid. The min-max method was used to normalize records to [0, 1] range. This was done to minimize the impact of outliers and maximize the classifiers' performance. Normalization was done as per the mathematical Equation (1):

$$X' = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (1)$$

Where X is feature's initial value, $X'$is normalized value, X_{min} is its minimum value, and $X_{max}$is its highest value.

2.4. Feature Extraction

The process of feature extraction transforms unprocessed network information into useful representations that may be utilized to identify irregularities. It records important statistical characteristics (e.g., number of packets, bandwidth, flow lifetime), as well as temporal characteristics (e.g., sequence of traffic and intervals of connections). Attributes based on protocol behavior that are content-based are also considered when determining malicious activity. This is further enhanced by high-level learning methods that learn space-association and sequence dependencies producing a sparse, informative feature set, which enhances detection accuracy and strength.

2.5. Data Splitting

In predictive analysis, dataset is split into two parts, 80% to train model and 20% to test. This plan ensures a successful learning process and enhances model's generalization ability in IoT.

2.6. Data Balancing using SMOTE

Cybersecurity Anomaly detection- The major challenges associated with class imbalance are one of the classes dominating the data, making the learning process biased and not able to identify the cases of minority. Synthetic Minority Oversampling Technique (SMOTE) can be employed to overcome this, which is a helpful method of data balancing. SMOTE synthesizes examples by interpolating between instances of the minority classes, increasing the diversity of the data, and ensuring the pattern is learned by the model in a balanced and representative way. This enhances the detectability, particularly of rare cyber-attacks. The distribution of the classes was indicated in Fig. 4 before and after SMOTE was used. To begin with, the samples of the dataset are skewed: there are more attack samples than there are normal samples. Following SMOTE, the two classes are balanced, which means that they are represented equally and enhances the strength and objectivity of training the ML models.

Fig 4: Bar graph of Class Distribution efore Vs after SMOTE of the Training Dataset

2.7. Proposed Model

The proposed model is the integration of CNNs and BiLSTM models, which can efficiently gather both temporal and geographical data to detect cybersecurity anomalies on the IoT with precision.

2.7.1. Convolutional Neural Network (CNN) Model

CNNs are DL systems that automatically extract characteristics from unprocessed data. CNNs in predictive maintenance and time-series analysis CNNs have been effectively used to learn local time-dependent patterns and fault-related patterns with convolutional kernels [25]. Shared weights mean that computational complexity is greatly decreased, and overfitting is avoided. The pooling layers improve strength by reducing noise and dimensionality. Stacked convolutional layers enable hierarchical learning of low- to high-level features. CNNs eliminate the need for handcrafted features. They improve generalization across varying operating conditions. Thus, CNNs provide discriminative representations for fault diagnosis.

$$y = f(W * x + b) \quad (2)$$

Equation (2) represents a convolution operation followed by a nonlinear activation function, forming the basis of CNN feature learning.

2.7.2. Bidirectional Long Short-Term Memory Network Model

The Bi-LSTM model leverages input data by precisely following its flow and efficiently captures temporal relationships in sequential data improvement. Both forward and reverse modules are included. Bi-LSTM networks with different topologies are used in their construction [26]. A weight, w, is associated with every action in the model. Data passes through both forward and backward hidden states during Bi-LSTM operation, producing a hidden layer output with bidirectional temporal processing. Equations (3)–(5)

display the status update of the forward and backward LSTM hidden layer as well as the BiLSTM final output process.

$$h_t = f_1(w_1 x_t + w_2 h_{t-1}) \quad (3)$$
$$h'_t = f_2(w_3 x_t + w_4 h'_{t+1}) \quad (4)$$
$$o_t = f_3(w_5 h_t + w_6 h'_t) \quad (5)$$

Where, activation functions across various levels are represented by f_1, f_2, and f_3, respectively (Equation 6).

$$f_t = \sigma\left(W_f[h_{t-1} x_t] + b_f\right) \quad (6)$$

The current layer's output gate ot and hidden state ht are depicted in Equations (7) to (8):

$$o_t = \sigma(W_o[h_{t-1} x_t] + b_o) \quad (7)$$
$$h_t = o_t tanh(C_t) \quad (8)$$

In this context, W and b stand for the training matrix's weights and biases, respectively. The nonlinear activation function represented by the symbol σ produces values.

2.7.3. Proposed Hybrid CNN-Bi-LSTM Model

The suggested hybrid CNN-BiLSTM model blends bidirectional temporal learning with convolutional feature extraction. CNN layers initially extract robust local features from raw sensor signals. An LSTM layer that can assess forward and backward sequences is given these qualities.

This bidirectional mechanism captures complete temporal context. The hybrid architecture improves understanding of degradation trends. It enhances prediction accuracy and model stability. The model minimizes the loss of information with time.

$$h_t = [h_t, h_t] \quad (9)$$

The combination of forward LSTM and backward LSTM results in Equation (9), allows the full representation of the temporal features. For this model's training, it used the Adam optimizer with 50 iterations, a learning rate of 0.001, and 64 batches. Regularization makes use of dropout and binary cross-entropy loss.

2.8. Evaluation Metrics

A variety of performance criteria were utilized to assess model's suitability. Preparing a confusion matrix—which displays the number of accurate and wrong classifications—was the first step in summarizing categorization results. Here it may see the primary statistical variables: TN, FN, TP, and FP. Rec, F1, acc, and prec are some of the common evaluation measures that were created from this data:

Accuracy: The proportion of accurately predicted instances by trained model to all instances in the dataset (input samples) [27]. It is given as Equation (10)-

$$Acc = \frac{\text{TP+TN}}{\text{TP+Fp+TN+FN}} \quad (10)$$

Precision: The ratio of accurately predicted positive cases to all positive occurrences is used to assess a model's accuracy. Accuracy shows classifier's accuracy in predicting positive classes is represented by Equation (11)-

$$Prec = \frac{\text{TP}}{\text{TP+FP}} \quad (11)$$

Recall: This measure is proportion of correctly anticipated positive events to all instances that should have turned out positive. It is expressed mathematically as Equation (12)-

$$Rec = \frac{\text{TP}}{TP+FN} \quad (12)$$

F1 score: It aids in balancing memory and precision by combining the harmonic mean of the two. Its range is [0, 1]. Mathematically, it is given as Equation (13)-

$$F1 - score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (13)$$

False Negative Rate (FNR): The FNR, which is computed in Equation (14) is a model incorrectly classifies a certain percentage of actual positive occurrences as negative.

$$FNR = \frac{\text{FN}}{TP+FN} \quad (14)$$

The measured outcomes according to these indicators are discussed and presented in the following section to show the work of the suggested system.

3. Results and Discussion

A benchmark dataset consisting of realistic normal and attack network traffic, suggested model is tested using UNSW-NB15 dataset. TensorFlow 2.15.0, Keras 2.15.0, Scikit-learn, and the Imbalanced-learn module are all used in Python version 3.10, respectively, to preprocess and class-balance with SMOTE, respectively. Experiments are run on Google Colab using GPUs. The suggested CNN–BiLSTM model's performance is displayed in Table II. Its 99.3% testing acc and 100 percent training accuracy are indicative of its ability to learn and generalize. The prec (97.6%), rec (97.8) and F1 (96.9) values of this model are balanced and stable, which means that the model has equal and balanced detection. The low FNR (4.2%), also demonstrates its effectiveness in decreasing the number of missed attacks and, therefore, it can be implemented in IoT cybersecurity systems.

Table 2: Classification Results of the Proposed Model for Anomaly Detection

Metric	CNN-BiLSTM
Training Accuracy	100.0
Testing Accuracy	99.3
Precision	97.6
Recall	97.8
F1-Score	96.9
False Negative Rate	4.2

Fig. 5 displays suggested CNN-BiLSTM model's overall anomaly-detection performance. Important evaluation measures are displayed such as training accuracy, test acc, prec, rec, F1 and FNR. The model is very accurate and precise, thus classifying well and with a low FNR which is crucial in the application of cybersecurity. The results confirm that the suggested approach is successful in identifying both benign and malicious traffic.

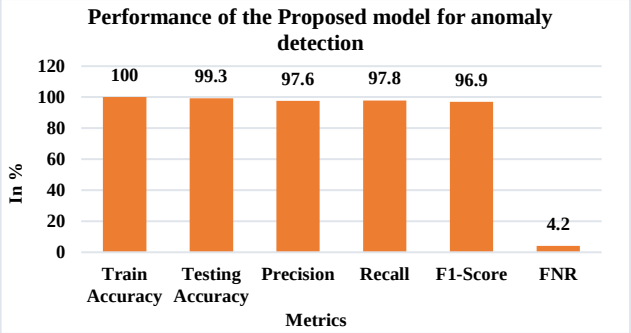

Fig 5: Performance Metrics of Proposed CNN–BiLSTM Model

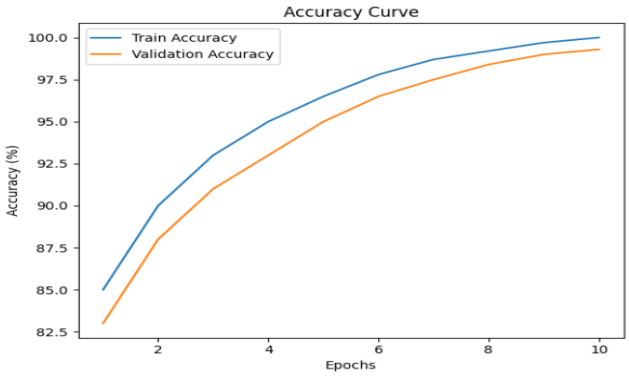

Fig 6: Accuracy Curve for the Proposed Model

The suggested model's training and validation accuracy trends are shown in Fig. 6 in terms of epochs. The two curves show a gradual rise, indicating that model is learning and converging. Strong generalization and mild over-fitting are shown by a small variation in accuracy between training and validation. The model quickly attains high accuracy in the initial epochs, and this indicates efficient learning of features on dataset, and behavior of optimization during the training is stable.

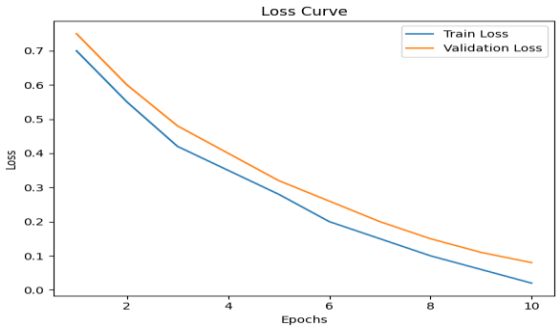

Fig 7: Loss Curve for Proposed Model

Fig. 7 shows loss decrease pattern of both training and validation data in epochs. The continuous decrease in loss demonstrates that the proposed model has been optimized. The fact that training and validation loss curves are close indicates stable learning and a lack of overfitting. The model converges smoothly, shows good parameter tuning and demonstrates strong learning ability. This demonstrates the model's reliability for cybersecurity anomaly detection in complex network environments.

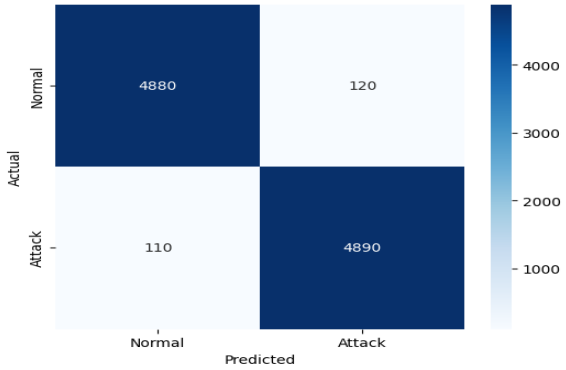

Fig 8: Confusion Matrix for the proposed Model

The classification performance of proposed model is shown by confusion matrix in Fig. 8. It shows both accurate and inaccurate forecasts for attack and regular classes. The model accurately predicts most cases, with 4880 normal and 4890 attack samples correctly classified. There are a few instances of misclassifications. This suggests considerable potential for identifying cybersecurity risks, excellent detection accuracy, and a low false alarm rate.

2.9. Comparative Analysis

The efficiency of various ML and DL models at identifying anomalies in IoT-based cybersecurity on benchmark datasets is shown in the comparative study in Table III, including TON_IoT, IoT Threat Data, BoT-IoT, and UNSW-NB15. To provide a clear and impartial assessment of each model's efficacy, the evaluation is conducted using commonly accepted performance criteria, such as acc, prec, rec, and F1. The findings demonstrate that conventional ML models, such LR and SVM, deliver reasonable performance but often lack consistency when applied to complex, large-scale IoT traffic data. In contrast, DL approaches such as Autoencoders and Deep Feedforward Neural Networks demonstrate improved learning ability by capturing more complex patterns in network behavior. Among all the compared models, the proposed Hybrid CNN-BiLSTM model achieves the best overall performance, with highest accuracy of 99.3%, as well as a high F1-score, recall, and accuracy. This clearly indicates its superior capability to learn features of IoT network traffic in both space and time, making it highly effective at detecting advanced and evolving cyber threats in intelligent IoT environments.

Table 3: Performance Comparison of Existing ML and Deep Learning Models for IoT-Based Cybersecurity Anomaly Detection

References	Model	Dataset	Accuracy	Precision	Recall	F1-score
[28]	MLP	TON_IoT Dataset	93.70	83	81	80
[29]	SVM	IoT threat data	96.5	95.9	96.2	96
[30]	Autoencoder	BoT IoT data	84.30	89	87	80

[31]	LR	UNSW-NB15 dataset	77.64	73.18	93.74	82.20
[32]	DFFNN	UNSW-NB15 dataset	97.54	96.58	97	96.9
Proposed	Hybrid CNN-BiLSTM	UNSW-NB15 dataset	99.3	97.6	97.3	96.9

2.10. Discussion

The results of the experiment demonstrate that suggested CNN-BiLSTM model achieves high rec, acc, and prec, showing a notable ability to distinguish between malicious and normal network data. Bidirectional temporal learning of convolutional layers enables model to effectively capture complex spatiotemporal patterns in IoT data. SMOTE also enhances detection performance for minority attack classes, minimizing classification bias. Nonetheless, there are some drawbacks. The model is computationally intensive and, therefore, might not be practical for resource-constrained edge devices. Furthermore, the test is conducted on a benchmark dataset that could not accurately represent a dynamic IoT environment in the real world. The model is also binary-based, which restricts its use for multi-class attacks. Despite these drawbacks, the framework has strong potential for real-world cybersecurity applications.

3. Conclusion and Future Study

A smart IoT-based DL model is developed to enhance cybersecurity by detecting anomalies with a hybrid CNN-BiLSTM architecture. The model learns temporal variations in network traffic data using bidirectional long short-term memory networks and efficiently extracts spatial characteristics using a CNN. The usefulness of proposed strategy is demonstrated on UNSW-NB15 dataset, where it outperforms existing DL techniques and conventional ML methods. The model's remarkable precision, recall, and F1-score, intrigate with its test accuracy of 99.3, reveal its high ability to distinguish between benign and malignant activity. Moreover, use of preprocessing methods such as normalization and SMOTE-based data balancing based on SMOTE improves system's strength and generalization capacity. The outcomes demonstrate model's ability to identify sophisticated cyberthreats and enhance IoT infrastructure security. The model can be further enhanced by deploying it in real-time edge scenarios to support low-latency IoT applications. Lightweight architectures and model optimization methods can be used to make resource-constrained devices more efficient. The practical use of the framework will also be improved by extending the classification to multi-class and acknowledging zero-day attacks. In addition, federated learning and blockchain-based security can be integrated to improve data privacy, scalability and resilience in distributed IoT ecosystems.

References

[1] B. N. I. S. Phalke and Y. D. Athave, "A Multi-Layered Approach to IT Infrastructure Governance and Compliance: Security, Hardening, and Audit Readiness," *Int. J. Comput. Appl.*, vol. 187, no. 12, p. 9, 2025.

[2] B. F. More and S. Pawar, "Smart Home System Using Iot," *Int. J. Manag. Technol. Eng.*, vol. 8, no. XI, p. 2241, 2018.

[3] S. H. A. Pushkala, V. K. Jammula, A. Chowdhury, D. Reboredo, and A. Shehata, "Method and system to predict network performance of a fixed wireless network," US12114185B2, Oct. 2024

[4] R. rao Thallada and N. Alapati, "Privacy and Cybersecurity Convergence: GRC Controls for Data Protection," *J. Bus. Manag. Stud.*, vol. 8, no. 5, pp. 42–48, March, 2026, doi: 10.32996/jbms.

[5] S. Priyadarshini, C. Althati, M. Tomar, K. R. Jinna, T. Pichaimani, and V. P. Rambabu, "A Scalable Digital Twin Architecture for Intelligent Cyber Physical Systems," in *2026 International Conference on Machine Learning and Autonomous Systems (ICMLAS)*, Bangkok, Thailand: IEEE, 2026, pp. 1841–1847, March. doi: 10.1109/ICMLAS67792.2026.11483673.

[6] S. K. Chintagunta, "Enhancing Cloud Database Security Through Intelligent Threat Detection and Risk Mitigation," *TIJER – Int. Res. J.*, vol. 9, no. 10, pp. 49–55, 2022.

[7] H. P. Cyril, "DeepNetDetect: A Deep Learning-Based Approach for Early Anomaly Detection in Network Traffic," in *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, IEEE, Feb. 2026, pp. 1–6. doi: 10.1109/ICAIC67076.2026.11395734.

[8] D. Bhattacharjee, "Design and Evaluation of Deep Generative AI Model for Intrusion Detection in Cyber Threat Monitoring," in *2025 7th International Symposium on Advanced Electrical and Communication Technologies (ISAECT)*, Mohali, Punjab, India: IEEE, 2025, pp. 1–6, December. doi: https://doi.org/10.1109/ISAECT68904.2025.11318752.

[9] V. Pal and S. Amrale, "Quantum-Resistant Federated Learning Framework for Secure IoT Networks with Lattice-Based Cryptography," in *2025 Seventh International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*, IEEE, Dec. 2025, pp. 343–350. doi: 10.1109/ICRCICN68210.2025.11364899.

[10] M. Kumar and M. K. Shah, "AI-Driven DDoS Detection for Network Security: A Performance Analysis of Machine-Deep Learning Methods on Network Traffic Data," in *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, Houston, TX, USA: IEEE, 2026, pp. 1–6, February. doi: 10.1109/ICAIC67076.2026.11395710.

[11] Naveen Kolli, John Wesly Sajja, Anusha Nerella, "Building Secure AI Agents for Autonomous Data Access in Compliance/Regulatory-Critical Environments," *Comput. Fraud Secur.*, pp. 363–373, 2024, doi: 10.52710/cfs.746.

[12] V. K. Sharma, "AI-Based Anomaly Detection for 5G Core and RAN Components," *Int. J. Sci. Res. Eng. Manag.*, vol. 6, no. 1, pp. 1–6, june, 2022, doi: 10.55041/IJSREM11453.

[13] R. Palwe, "Three Layers of Trust in AI Interfaces: Interface, Behavior, and Organization," *Int. J. Sci. Res.*, vol. 15, no. 1, pp. 1152–1160, Jan. 2026, doi: 10.21275/SR26112072531.

[14] R. Dattangire, R. Vaidya, D. Biradar, and A. Joon, "Exploring the Tangible Impact of Artificial Intelligence and Machine Learning: Bridging the Gap between Hype and Reality," in *2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET)*, 2024, pp. 1–6. doi: 10.1109/ACET61898.2024.10730334.

[15] K. K. Mohammed, "Leadership Practices of Data Engineering for AI and Machine Learning," *Int. J. Sci. Res. Eng. Trends*, vol. 12, no. 1, pp. 1–5, 2026.

[16] P. Nutalapati, J. R. Vummadi, S. Dodda, and N. Kamuni, "Advancing Network Intrusion Detection: A Comparative Study of Clustering and Classification on NSL-KDD Data," in *2025 International Conference on Data Science and Its Applications (ICoDSA)*, Jakarta, Indonesia: IEEE, 2025, pp. 880–885, july. doi: 10.1109/ICoDSA67155.2025.11157595.

[17] A. R. Toorpu, S. K. Vududala, A. Nerella, and B. P. Madupati, "Hybrid AI Models for Privacy-Preserving Big Data Analytics in Distributed Environments," in *2025 Global Conference in Emerging Technology (GINOTECH)*, PUNE, India: IEEE, 2025, pp. 1–8, July. doi: 10.1109/GINOTECH63460.2025.11076666.

[18] S. Sudheer, "Data Engineering for Dynamic and Secure Blockchain Networks in AI Applications," *Int. J. Inf. Electron. Eng.*, vol. 13, no. 4, pp. 52–61, May, 2025, [Online]. Available: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=kKQadycAAAAJ&citation_for_view=kKQadycAAAAJ:SeFeTyx0c_EC

[19] S. Manekar, "An Intelligent Deep Learning Framework for Anomaly Detection in IoT Cybersecurity," *J. Artif. Intell. Healthc. FinTech Syst.*, vol. 1, no. 1, pp. 23–29, 2026.

[20] M. P. K, D. Marotka, M. J, R. Adhvaryu, V. V, and R. Maranan, "Traffic Surveillance System Through Capsule Gated Graph Attention Network for IoT/IIoT Cyberthreat Detection and Mitigation," in *2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS)*, IEEE, Mar. 2025, pp. 1974–1980. doi: 10.1109/ICMLAS64557.2025.10968575.

[21] S. Aslam, M. M. R. Alshoweky, and M. Saad, "Binary and Multiclass Classification of Attacks in Edge IIoT Networks," in *2024 Advances in Science and Engineering Technology International Conferences (ASET)*, IEEE, Jun. 2024, pp. 01–05. doi: 10.1109/ASET60340.2024.10708745.

[22] X. Li, C. Xie, Z. Zhao, C. Wang, and H. Yu, "Anomaly Detection Algorithm of Industrial Internet of Things Data Platform Based on Deep Learning," *IEEE Trans. Green Commun. Netw.*, vol. 8, no. 3, pp. 1037–1048, Sep. 2024, doi: 10.1109/TGCN.2024.3403102.

[23] S. Chakraborty, S. K. Pandey, S. Maity, and L. Dey, "Detection and Classification of Novel Attacks and Anomaly in IoT Network using Rule based Deep Learning Model," *SN Comput. Sci.*, vol. 5, no. 8, p. 1056, Nov. 2024, doi: 10.1007/s42979-024-03429-5.

[24] L. Zhao, B. H. Li, J. Jia, and T. Wu, "Anomaly Detection Technology for Cloud Manufacturing System based on Data Denoising and Feature Optimization," in *ICNSC 2022 - Proceedings of 2022 IEEE International Conference on Networking, Sensing and Control: Autonomous Intelligent Systems*, 2022. doi: 10.1109/ICNSC55942.2022.10004139.

[25] D. Jain and S. Jain, "Artificial Intelligence (AI)-Driven Network Traffic Anomaly Detection for IT Infrastructure Security," in *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, IEEE, Feb. 2026, pp. 1–6. doi: 10.1109/ICAIC67076.2026.11395685.

[26] H. Nandanwar and R. Katarya, "TL-BILSTM IoT: transfer learning model for prediction of intrusion detection system in IoT environment," *Int. J. Inf. Secur.*, vol. 23, no. 2, pp. 1251–1277, 2024.

[27] B. Madupati, M. M. Mohammed, L. Upadhyay, D. P. Guda, K. Kaushik, and M. Soni, "Integrating Artificial Intelligence with Cybersecurity for Resilient Wireless Communication Against Advanced Threats," in *2025 International Conference on Artificial Intelligence and Machine Vision (AIMV)*, IEEE, Aug. 2025, pp. 1–5. doi: 10.1109/AIMV66517.2025.11203666.

[28] A. Javed, A. Ehtsham, M. Jawad, M. N. Awais, A.-H. Qureshi, and H. Larijani, "Implementation of Lightweight Machine Learning-Based Intrusion Detection System on IoT Devices of Smart Homes," *Futur. Internet*, vol. 16, no. 6, p. 200, Jun. 2024, doi: 10.3390/fi16060200.

[29] M. Gopalswamy, "Building Scalable Anomaly Identification Systems to IoT Threat Mitigation using Machine learning Techniques," *J. Glob. Res. Math. Arch.*, vol. 12, no. 1, 2025, doi: 10.5281/zenodo.15201777.

[30] N. Sarwar, I. S. Bajwa, M. Z. Hussain, M. Ibrahim, and K. Saleem, "IoT Network Anomaly Detection in Smart Homes Using Machine Learning," *IEEE Access*, vol. 11, pp. 119462–119480, 2023, doi: 10.1109/ACCESS.2023.3325929.

[31] S. M. Kasongo and Y. Sun, "Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset," *J. Big Data*, vol. 7, no. 1, 2020, doi: 10.1186/s40537-020-00379-6.

[32] F. Lawrence and R. Nigam, "High-Accuracy Intrusion Detection System using Deep Learning Ensembles and Reinforcement Learning on the NF-UNSW-NB15 Dataset," *J. Informatics Educ. Res.*, vol. 5, no. 4, pp. 173–199, 2025.