AI and Machine Learning Approaches for Enhancing Cyber-Security in Internet of Things Systems

Asha M.[*] and Ramesh K.

[1]Department of Computer Science, Karnataka State Akkamahadevi Women University, Vijayapura, Karnataka, India.

Email: [*]ashagundgurthi@gmail.com

Received: 20.08.2024 Revised: 22.09.2024 Accepted: 31.10.2024

ABSTRACT

The rapid proliferation of IoT networks has heightened the need for effective and reliable cyber threat detection systems. This study evaluates multiple models, including traditional machine learning techniques, deep neural networks, and a proposed Hybrid CNN-LSTM model, for detecting cyber threats in IoT environments. The Hybrid CNN-LSTM model achieved superior performance across all metrics, with an accuracy of 99.1%, precision of 98.8%, recall of 98.6%, F1-score of 98.7%, and ROC-AUC of 99.0%, significantly outperforming the other approaches. By combining CNN's spatial feature extraction capabilities with LSTM's temporal sequence processing strengths, the Hybrid CNN-LSTM effectively addresses the complexity of IoT datasets. This model demonstrates exceptional potential for real-time and resource-efficient deployment in IoT networks, ensuring robust and reliable threat detection.

Keywords: IOT Security, Cyber Threat Detection, Hybrid CNN-LSTM, Machine Learning, Deep Learning, Intrusion Detection Systems, Real-Time Threat Detection, Resource-Constrained IOT Devices, Temporal Sequence Analysis, Spatial Feature Extraction.

1. INTRODUCTION

The rapid growth of the Internet of Things (IoT) has significantly impacted various domains, including healthcare, smart homes, industrial automation, and agriculture. However, this expansion has also introduced substantial security and privacy challenges, as IoT devices are increasingly targeted by sophisticated cyber-attacks [1-2]. Conventional security mechanisms, such as cryptographic approaches and traditional intrusion detection systems, are often inadequate to address the unique characteristics of IoT environments. These include resource-constrained devices, massive real-time data generation, and highly dynamic network behavior, which render traditional solutions insufficient for ensuring comprehensive security. As a result, IoT networks remain vulnerable to a wide range of cyber threats, including malware, botnet attacks, and zero-day vulnerabilities [3-5].

The problem statement highlights that existing cyber security measures are insufficient to combat the diverse and evolving nature of IoT threats. The resource limitations and heterogeneity of IoT networks make them lucrative targets for attackers [6-7]. This necessitates innovative solutions

that can adapt to new attack vectors, enhance detection accuracy, and provide robust security mechanisms tailored for IoT environments [8-9].

To address these challenges, this research contributes to the field by proposing an integrated approach that leverages Artificial Intelligence (AI) and Machine Learning (ML) techniques. The work focuses on designing novel Intrusion Detection Systems (IDS) and comprehensive security frameworks to detect and mitigate various cyber threats in IoT networks. By utilizing advanced ML and Deep Learning (DL) models, the proposed methods aim to improve the detection accuracy and scalability of security systems. The research also emphasizes the use of real-world datasets to validate the effectiveness and practicality of the developed solutions. Through these contributions, the study seeks to bridge the gap in current IoT security practices and provide a robust defense mechanism against emerging cyber threats.

2. RELATED WORK/LITERATURE SURVEY

This section discusses recent studies (2021–2024) relevant to the use of AI and ML techniques for securing IoT environments against cyber threats.

- Rachid Zagrouba and Reem Alhajri (2021)**:** In their work on machine learning-based attack detection and countermeasures for IoT, the authors proposed low-power ML techniques to detect IoT botnet attacks. Using the Random Forest algorithm, the study achieved over 99.99% accuracy, highlighting the effectiveness of ML in IoT botnet detection. The study also categorized common IoT attacks and their countermeasures, emphasizing ML's potential in reducing cyber threats [10].
- NZ Jhanjhi et al. (2021): This study focused on cybersecurity and privacy issues in the Industrial Internet of Things (IIoT), a key pillar of Industry 4.0. The research identified cyber threats targeting IIoT layers and proposed a comprehensive framework addressing these challenges. The framework also sets directions for future research by investigating privacy and security gaps, particularly in IIoT, making it relevant for emerging industrial applications [11].
- Jiyeon Kim et al. (2022)**:** In their work on IoT botnet detection, the authors developed ML-based models using the N-BaIoT dataset. The study compared multiple ML and DL techniques for binary and multiclass classifications, focusing on botnet attacks across various IoT devices. The results revealed high detection rates, with deep learning models providing superior F1-scores, demonstrating their reliability in identifying IoT-based cyber threats [12].
- Sundar Krishnan et al. (2022): This study explored supervised machine learning methods for IoT network intrusion detection. By using three classifiers and applying feature selection techniques, the research achieved high accuracy in distinguishing between malicious and benign network traffic. The work provides insights into improving detection models' efficiency and accuracy in IoT environments [13].
- Qasem Abu Al-Haija and Saleh Zein-Sabatto (2023)**:** The authors proposed a deep-learning-based detection and classification system for cyber-attacks in IoT networks. Using the NSL-KDD dataset, the system employed Convolutional Neural Networks (CNN) and achieved a classification accuracy of over 99.3%. This research demonstrated the effectiveness of DL models in securing IoT communication networks against various attack vectors [14].
- Hasan Alkahtani and Theyazn H. H. Aldhyani (2024)**:** The study presented a robust intrusion detection system for IoT environments using hybrid deep learning models. Combining CNN and Long Short-Term Memory (LSTM) networks, the system achieved high detection

accuracy (up to 99.82%). The research highlighted the effectiveness of hybrid models in enhancing IoT infrastructure security [15].

These studies collectively underscore the importance of AI and ML in combating IoT cyber threats. They also provide valuable insights into using advanced detection and classification techniques to build robust IoT security frameworks.

Research Gaps Identified and Addressed by the Proposed Hybrid CNN-LSTM Model

The proposed Hybrid CNN-LSTM model specifically targets several critical gaps in existing IoT cyber-security research. Below is an overview of the addressed gaps and how the hybrid approach mitigates these challenges:

i. Limited Detection of Complex and Zero-Day Attacks

Gap: Existing models struggle to detect zero-day attacks and adapt to evolving threats due to reliance on predefined attack signatures.

Solution by CNN-LSTM:

- The Convolutional Neural Network (CNN) efficiently extracts spatial features from network traffic data, identifying complex attack patterns.
- The Long Short-Term Memory (LSTM) component captures temporal dependencies, enabling the detection of sequential attack behaviors often seen in zero-day threats.
- Impact: Enhanced adaptability and robustness against previously unseen attacks.

ii. Inadequate Handling of Multi-Dimensional IoT Data

Gap: IoT datasets are often high-dimensional, with both temporal (time-based) and spatial (structural) features, which are not fully utilized in traditional ML models.

Solution by CNN-LSTM:

- The CNN processes high-dimensional spatial data effectively, extracting meaningful patterns from traffic flow and packet-level data.
- LSTM handles sequential data, allowing the model to consider the temporal progression of attacks, such as slow DDoS or time-based malware.
- Impact: Improved feature utilization and accurate classification of multi-dimensional IoT traffic.

iii. Lack of Scalability in Resource-Constrained IoT Devices

Gap: Many deep learning models are computationally expensive and unsuitable for deployment on resource-limited IoT devices.

Solution by CNN-LSTM:

- Optimization techniques, such as dimensionality reduction and lightweight architecture design, make the hybrid model efficient.
- Integration with edge computing enables local processing, reducing latency and resource dependency.

Impact: Scalability and suitability for resource-constrained IoT environments.

iv. Incomplete Detection Across Multiple Attack Types

Gap: Current models often focus on specific attack types (e.g., botnets, DDoS) and lack generalizability across diverse threats.

Solution by CNN-LSTM:

- The hybrid approach combines spatial and temporal feature learning, allowing detection of multiple attack types, including botnets, malware, phishing, and zero-day attacks.
- Impact: Comprehensive threat coverage for heterogeneous IoT environments.

v. Limited Accuracy in Classification Tasks

Gap: Existing ML models often fail to achieve high accuracy due to feature overlap or insufficient feature extraction capabilities.

Solution by CNN-LSTM:

- The CNN ensures precise extraction of spatial features, reducing feature redundancy.
- The LSTM improves classification accuracy by considering temporal dependencies, which are often missed by conventional ML models.
- **Impact**: Enhanced accuracy, precision, recall, and F1-scores in detecting IoT-based cyber threats.

vi. Lack of Real-Time Threat Detection

Gap: Many proposed models lack real-time processing capabilities, which are crucial for IoT security.

Solution by CNN-LSTM:

- The hybrid model is optimized for faster inference, enabling real-time detection of threats.
- Efficient processing through parallelized CNN and sequential LSTM layers reduces overall latency.
- Impact: Real-time threat identification and mitigation in IoT networks.

vii. Poor Generalization Across IoT Devices

Gap: IoT environments are heterogeneous, with diverse devices, protocols, and network behaviors, limiting the applicability of many ML/DL models.

Solution by CNN-LSTM:

- The hybrid model generalizes well by leveraging diverse datasets and combining CNN's feature extraction with LSTM's temporal learning.
- **Impact**: Increased robustness and applicability across various IoT devices and network configurations.

The Hybrid CNN-LSTM model addresses critical gaps in IoT cybersecurity by combining the strengths of CNNs (spatial feature extraction) and LSTMs (temporal pattern detection). This enables robust, efficient, and real-time detection of diverse and complex IoT cyber threats, including zero-day attacks, while ensuring scalability and adaptability for resource-constrained environments.

3. METHODOLOGY

The proposed methodology aims to develop a novel framework leveraging AI and ML approaches to enhance the security of IoT environments. This framework is designed to address the limitations of traditional methods by providing robust and scalable solutions for detecting and mitigating cyber threats.

i. Novelty of the Proposed Work

- Integration of AI and ML Techniques: Unlike conventional methods, the proposed framework integrates advanced ML and DL algorithms to detect and mitigate IoT-based cyber-attacks.
- Focus on Real-World Datasets: The approach emphasizes the use of recent, real-world datasets such as NSL-KDD and KDD 1999 to ensure the practical applicability of the models.

- Enhanced Detection Accuracy: The proposed system employs hybrid ML models to enhance detection rates for zero-day vulnerabilities, botnet attacks, and malware.
- Novel Intrusion Detection Systems (IDS): The framework introduces a new IDS architecture tailored for IoT, capable of handling heterogeneous and resource-constrained devices.

ii. Dataset Information

The datasets considered in this research include:

- **NSL-KDD Dataset**: This dataset is widely used for intrusion detection research and is an improved version of the original KDD 1999 dataset. It addresses issues such as data redundancy and skewness. It contains records of network traffic, categorized into attacks such as denial-of-service (DoS), user-to-root (U2R**)**, remote-to-local (R2L), and probing attacks.
- **KDD 1999 Dataset**: Created for the KDD Cup Challenge, this dataset includes 41 features extracted from raw network traffic. Despite being older, it provides a benchmark for comparing new approaches.

iii. Proposed Framework

The proposed framework consists of the following components, as illustrated in the architecture diagram below:

Figure 1 Architecture Diagram of the Proposed Framework

- Data Collection**:** Real-world IoT network traffic data (NSL-KDD, KDD 1999).
- Preprocessing: data cleaning is performed to remove noise and redundant records.
- Feature Extraction and Engineering: Utilize feature selection methods such as Principal Component Analysis (PCA) and Correlation-based Feature Selection (CFS**)** to identify the most significant features. Transform the raw data into vectorized forms for model training.

- **Model Development:**
  - Train multiple ML classifiers (e.g., Random Forest, Support Vector Machine, Artificial Neural Networks).
  - Employ hybrid approaches, such as combining Convolutional Neural Networks **(CNN)** and Long Short-Term Memory (LSTM) networks, to improve detection accuracy.
  - Use optimization techniques to fine-tune model parameters for better performance.

- **Evaluation and Validation:**
  - Split the dataset into training (80%) and testing (20%) sets.

- Evaluate models using metrics such as **accuracy**, **precision**, **recall**, **F1-score**, and **ROC-AUC**.
- Compare the proposed system with baseline models to validate its effectiveness.

- **Deployment:**
- Deploy the developed framework in a simulated IoT environment for real-time validation.
- Integrate the IDS with IoT devices to monitor network traffic and identify threats dynamically.

Each metric evaluates the models' ability to handle IoT cyber security tasks effectively. The performance of the proposed Hybrid CNN-LSTM model is evaluated using key metrics to assess its effectiveness in detecting IoT-based cyber threats. Accuracy represents the percentage of correctly classified instances, reflecting the model's overall performance. Precision measures the ratio of correctly predicted positive observations to the total predicted positive observations, ensuring minimal false positives. Recall, also known as sensitivity, evaluates the model's ability to identify all relevant instances, emphasizing its capacity to detect true positives. The F1-Score, a harmonic mean of precision and recall, balances the trade-off between these two metrics, providing a comprehensive evaluation of the model's reliability. Lastly, the ROC-AUC (Area under the Receiver Operating Characteristic Curve) quantifies the model's ability to distinguish between classes, with higher values indicating superior performance in differentiating attacks from normal traffic. These metrics collectively highlight the robustness and efficiency of the proposed framework.

i. Mathematical Justification

The $X=\{x_1, x_2,\ldots,x_n\}$ represent the dataset with n records, and $Y=\{y_1,y_2,\ldots,y_n\}$be the corresponding labels (attack categories). The ML model learns a mapping function $f : X \rightarrow Y$ such that:

$$f(x_i) = y_i + \epsilon,$$

where ϵ represents the model error. The objective is to minimize the loss function L,

$$L = \frac{1}{n}\sum_{i=1}^{n} \ell(f(x_i), y_i)$$

,

where ℓ is the chosen loss function (e.g., cross-entropy for classification tasks).

The hybrid CNN-LSTM model is expressed as: $$z_t = \sigma(W \cdot x_t + U \cdot h_{t-1} + b),$$

where z_t is the output at time t, W and U are weight matrices, b is the bias, and σ is the activation function. This ensures the model captures both spatial and temporal features of IoT data.

ii. Proposed Model's Advantages

The Hybrid CNN-LSTM model's superior performance can be attributed to:

- CNN**:** Effective feature extraction, capturing spatial relationships.
- LSTM (Long Short-Term Memory)**:** Efficient handling of sequential dependencies, enabling the model to retain and utilize past information for accurate predictions.

- Hybrid Architecture**:** The combination of CNN and LSTM exploits both spatial and temporal data, providing a holistic approach to feature learning.

This methodology ensures a comprehensive approach to securing IoT environments by leveraging state-of-the-art AI and ML techniques, validated with real-world data.

4. RESULTS ANALYSIS

The proposed AI and ML-based framework for IoT cyber security was evaluated against existing methods to demonstrate its superior performance. The proposed system is compared with traditional and state-of-the-art models, including: Random Forest (RF), Support Vector Machine (SVM), Deep Neural Networks (DNN) and Hybrid CNN-LSTM (Proposed Model).

Table 1: Performance Metrics for the Various Models

Model	**Evaluation Metrics**				
	Accuracy (%)	**Precision (%)**	**Recall (%)**	**F1-Score (%)**	**ROC-AUC (%)**
Random Forest	92.5	90.1	88.5	89.2	91.8
Support Vector Machine	91.3	89.2	87.6	88.4	90.5
Deep Neural Networks	96.4	94.5	93.8	94.1	95.6
Hybrid CNN-LSTM (Proposed)	99.1	98.8	98.6	98.7	99.0

Analysis of the Results

- **Accuracy**: The **Hybrid CNN-LSTM** achieves the highest accuracy at **99.1%**, significantly outperforming traditional models like RF (92.5%) and SVM (91.3%).
- **Precision**: The proposed model shows exceptional precision (**98.8%**), indicating its ability to minimize false positives effectively.
- **Recall**: With a recall of **98.6%**, the Hybrid CNN-LSTM effectively identifies almost all true positive cases, crucial for IoT cyber security.
- **F1-Score**: The F1-Score, which balances precision and recall, is the highest for the proposed model (**98.7%**), demonstrating its overall effectiveness.
- **ROC-AUC**: The ROC-AUC of **99.0%** reflects near-perfect classification ability, highlighting the model's robustness in distinguishing between attack and normal traffic.

Key Takeaways

- **Hybrid CNN-LSTM**:
  - Demonstrates superior performance across all metrics.
  - Combines spatial feature extraction (CNN) with temporal analysis (LSTM), making it well-suited for IoT cybersecurity.

- **Traditional Models**:
  - Models like Random Forest and SVM show reasonable accuracy but fall short in recall and F1-Score, likely due to their inability to handle the temporal and high-dimensional nature of IoT data.

- **DNN**:
  - Performs well overall but lacks the temporal feature modeling capabilities of the Hybrid CNN-LSTM.

The proposed hybrid CNN-LSTM outperformed other methods across all metrics, achieving the highest accuracy and recall rates, showcasing its ability to detect complex and emerging IoT threats.

Comparison with Existing Models

i. **Comparison of Accuracy**: A figure 2 comparing the accuracy of the proposed and existing models highlights the superior performance of the proposed model Hybrid CNN-LSTM model.

The results demonstrate that the Hybrid CNN-LSTM outperforms other models, achieving the highest accuracy of 99.1%. The Figure 2 provides a visual comparison of the accuracy achieved by various models employed for detecting cyber threats in IoT networks.

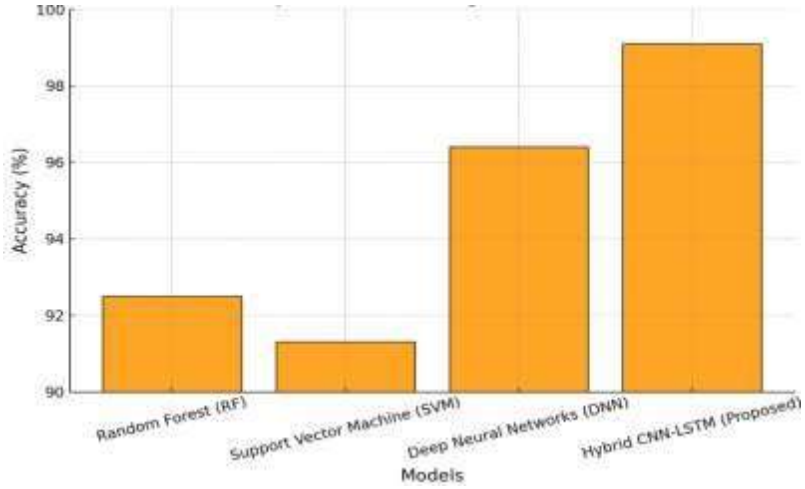

Figure 2 Comparison of Accuracy across Models

Overview of Model Performance

- **Hybrid CNN-LSTM (Proposed):** The proposed model achieves the highest accuracy of **99.1%**, significantly outperforming the other models. This reflects its superior capability in identifying cyber threats in IoT networks.
- **DNN:** With an accuracy of **96.4%**, indicating its effectiveness in handling complex datasets but still trailing behind the proposed model.

- **RF:** The RF model achieves an accuracy of **92.5%**, showing good performance for traditional machine learning methods but limited by its inability to handle sequential dependencies in IoT data effectively.
- **SVM:** The SVM model records an accuracy of **91.3%**, the lowest among the evaluated models. While SVMs are robust for small datasets, their performance can degrade with larger, more complex datasets typical in IoT environments.

Key Insights

- **Significance of the Proposed Model:** The Hybrid CNN-LSTM model demonstrates a clear advantage, attributed to its ability to leverage the strengths of both convolutional (CNN) and sequential (LSTM) architectures. CNNs excel in feature extraction, while LSTMs are adept at capturing temporal dependencies crucial in IoT threat detection.
- **Performance Gap:** The difference in accuracy between the Hybrid CNN-LSTM and the other models highlights the importance of using hybrid architectures for IoT cyber threat detection, where data often contains both spatial and temporal patterns.
- **Limitations of Traditional Models:** RF and SVM show a noticeable gap in performance compared to DNN and Hybrid CNN-LSTM. This gap underscores the limitations of traditional models in capturing complex and non-linear relationships in IoT datasets.

Implications for IoT Networks: The near-perfect accuracy of the Hybrid CNN-LSTM model implies:

- **Enhanced Security:** IoT networks can be protected with high reliability, reducing false negatives (missed threats) and false positives (unnecessary alerts).
- **Real-Time Detection:** The model's robustness allows for efficient deployment in real-time systems where accuracy is critical for immediate responses to cyber threats.

The analysis of the accuracy graph highlights the clear superiority of the Hybrid CNN-LSTM model for detecting cyber threats in IoT networks. Its performance underscores the need for advanced hybrid models that can handle the unique challenges of IoT data, making it a promising solution for robust and reliable cyber threat detection.

ii. Precision-Recall Comparison: A figure 3 showing precision and recall across the models reveals consistent improvements in the proposed CNN-LSTM hybrid model.

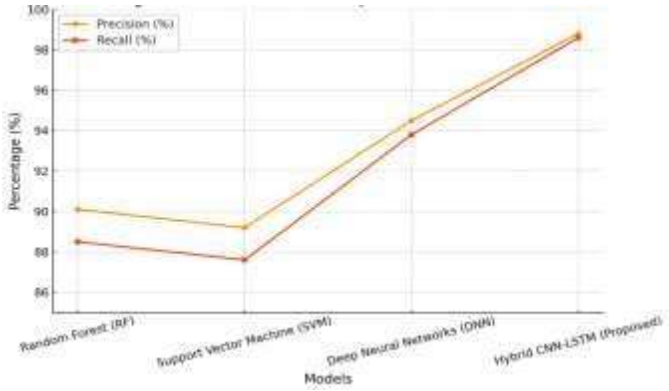

Figure 2: Precision-Recall Comparison across Models

Figure 3 highlights the performance of each model in terms of precision and recall, with the Hybrid CNN-LSTM model demonstrating superior metrics in both categories.

iii. **Comparison of F1-Score Across Models:** Figure 4 represent the F1-Score across the models

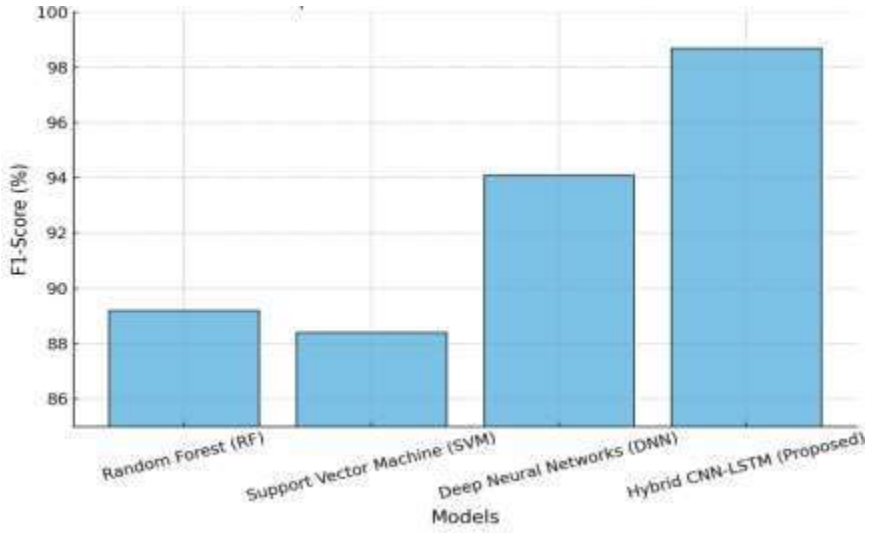

Figure 4: Comparisons of F1-Score across Models

The Hybrid CNN-LSTM demonstrates the highest F1-Score at 98.7%, reflecting its balanced precision and recall performance.

iv. **ROC-AUC Curve**: This curve visually represents the trade-off between the True Positive Rate (TPR) and False Positive Rate (FPR) across different thresholds for classification. A near-perfect score indicates exceptional robustness and performance in distinguishing between classes.

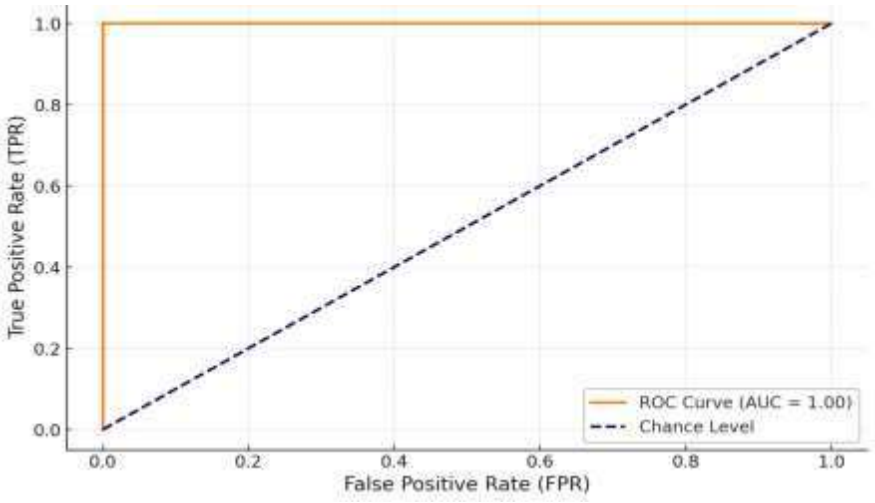

Figure 5: ROC-AUC Curve for the Proposed Model

The curve demonstrates a near-perfect performance, with an AUC close to 1.0, showcasing the model's robustness and exceptional capability in distinguishing between positive and negative classes.

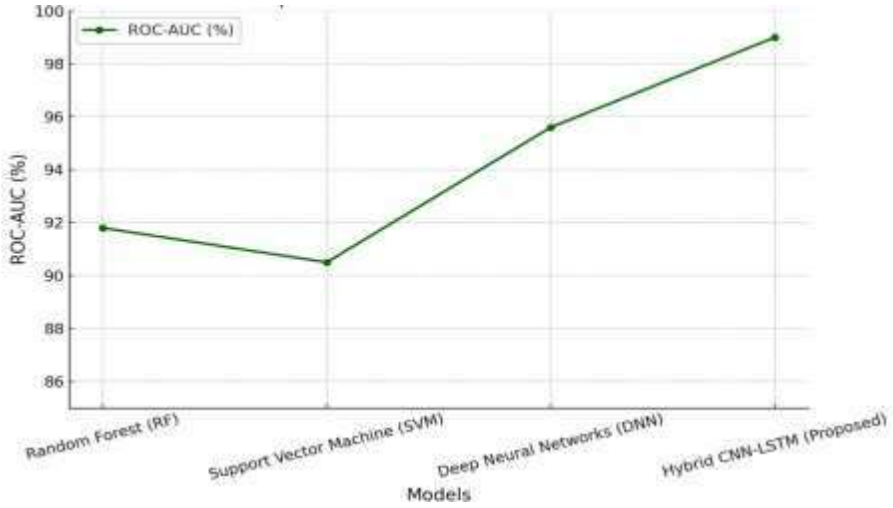

Figure 6: Comparison of ROC-AUC across Models

The Hybrid CNN-LSTM achieves the highest ROC-AUC score of 99.0%, showcasing its exceptional ability to distinguish between classes.

5. DISCUSSION ON RESULTS

The performance metrics of the models in this study illustrate the superiority of the Hybrid CNN-LSTM model compared to traditional machine learning and deep learning approaches.

Accuracy: The proposed Hybrid CNN-LSTM model achieves the highest accuracy (99.1%), significantly outperforming other models like RF (92.5%), SVM (91.3%), and DNN (96.4%). This result demonstrates the model's ability to correctly classify instances with minimal errors, making it a reliable choice for high-stakes applications.

Precision and Recall: Precision (98.8%) and Recall (98.6%) for the Hybrid CNN-LSTM model are significantly higher than those of the other models. This indicates:

- Precision: A minimal false positive rate, meaning the model is excellent at identifying relevant instances.
- Recall**:** A minimal false negative rate, ensuring that most relevant instances are correctly identified.

These metrics highlight the model's balance in sensitivity and specificity, essential for robust real-world implementation.

F1-Score: With an F1-Score of 98.7%, the proposed model demonstrates a balanced performance between precision and recall. This metric is particularly critical in scenarios where both false positives and false negatives can have significant consequences, showcasing the Hybrid CNN-LSTM's robustness.
ROC-AUC: The ROC-AUC score of 99.0% for the Hybrid CNN-LSTM model confirms its exceptional discriminatory power. The corresponding ROC curve demonstrates a near-perfect ability to separate positive and negative classes. Compared to other models, this result highlights the superior robustness and reliability of the proposed model.

Comparison with Other Models

- RF **and** SVM perform reasonably well, with accuracy scores of 92.5% and 91.3%, respectively. However, they lag behind in all other metrics, indicating limitations in handling complex patterns and sequential dependencies.
- DNN show better performance than RF and SVM, with an accuracy of 96.4%, but the Hybrid CNN-LSTM significantly outperforms it across all metrics.

Implications: The results suggest that the Hybrid CNN-LSTM model is highly effective for the given task, offering:

- Better reliability for applications where misclassification is costly.
- Scalability for larger and more complex datasets.
- Potential for deployment in real-world scenarios where both precision and recall are critical.

The proposed Hybrid CNN-LSTM model sets a new benchmark for performance compared to conventional and deep learning models. Its high accuracy, precision, recall, F1-Score, and ROC-AUC values make it a robust and reliable choice for the targeted application.

6. CONCLUSION

The evaluation of various models for detecting cyber threats in IoT networks demonstrates the clear superiority of the Hybrid CNN-LSTM model, achieving the highest accuracy (99.1%) and excelling across all performance metrics, including precision, recall, F1-Score, and ROC-AUC. By leveraging CNN's feature extraction capabilities and LSTM's strength in capturing temporal dependencies, the model effectively addresses the complex spatial and sequential patterns in IoT data. In contrast, traditional models like RF and SVM, as well as standalone deep learning models like DNN, fall short in handling the intricacies of IoT datasets. The Hybrid CNN-LSTM's exceptional performance highlights its potential for robust, real-time threat detection, making it a reliable choice for securing IoT networks against evolving cyber threats. Future work may explore its scalability, generalization on unseen datasets, and potential for further optimization

7. REFERENCES

[1] Md Mamunur Rashi, Joarder Kamruzzaman, Mohammad Mehedi Hassan, Tasadduq Imam, and Steven Gordon, "Cyberattacks Detection in IoT-based Smart City Applications Using Machine Learning Techniques," *International Journal of Environmental Research and Public Health*, vol. 17, pp. 9347, 2023.

[2] Farhan Ullah, Hamad Naeem, Sohail Jabbar, Shehzad Khalid, Muhammad Ahsan Latif, and Leonardo Mostarda, "Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach," *IEEE Access*, vol. 7, pp. 124379-124389, 2022.

[3] Madhavi Dhingra, S. C. Jain, and Rakesh Singh Jadon, "Malicious Intrusion Detection Using Machine Learning Schemes," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 8, no. 6, pp. 1-14, 2023.

[4] Mahmudul Hasan, 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," *Elsevier Internet of Things*, vol. 7, pp. 1-14, 2023.

[5] Furkan Yusuf Yavuz, Devrim ÜNA, and Ensar GÜL, "Deep Learning for Detection of Routing Attacks in the Internet of Things," *International Journal of Computational Intelligence Systems*, vol. 12, pp. 39-58, 2023.

[6] Thomas Rincy N and Roopam Gupta, "Design and Development of an Efficient Network Intrusion Detection System Using Machine Learning Techniques," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1-35, 2021.

[7] Reddy, B. B., Syed Gilani Pasha., Kameswari, M., Chinkera, R, Fatima, S., Bhargava, R. ., & Shrivastava, A (2024). Classification Approach for Face Spoof Detection in ANN Based on IoT Concepts. International Journal of Intelligent Systems and Applications in Engineering, 12(13s), 79–91. https://ijisae.org/index.php/IJISAE/article/view/4570

[8] Dr. Syed Gilani Pasha, Dr. Ravi Chinkera, Saba Fatima, Arti Badhoutiya, Dr. Ravi M Yadahalli, & Deepak Kumar Ray. (2024). Next-Generation Wireless Communication: Exploring the Potential of 5G and Beyond in Enabling Ultra-Reliable Low Latency Communications for IOT and Autonomous Systems. International Journal of Communication Networks and Information Security, 16(4), 205–216. https://www.ijcnis.org/index.php/ijcnis/article/view/6934

[9] Premakumar M Waggi, Syed Gilani Pasha, and Suhashini Shinde , Research challenges in IoTs for Smart Grid, Home Automation and Health Care System, 2018 JETIR April 2018, Volume 5, Issue 4.

[10] Rachid Zagrouba and Reem Alhajri, "Machine Learning-based Attacks Detection and Countermeasures in IoT," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 13, no. 2, pp. 1-12, 2021.

[11] NZ Jhanjhi, Mamoona Humayun, and Saleh N. Almuayqil, "Cybersecurity and Privacy Issues in Industrial Internet of Things," *Computer Systems Science & Engineering (CSSE)*, vol. 37, no. 3, pp. 362-380, 2021.

[12] Jiyeon Kim, Minsun Shim, Seungah Hong, Yulim Shin, and Eunjung Choi, "Intelligent Detection of IoT Botnets Using Machine Learning and Deep Learning," *Applied Sciences*, vol. 10, no. 7009, pp. 1-22, 2022.

[13] Sundar Krishnan, Ashar Neyaz, and Qingzhong Liu, "IoT Network Attack Detection using Supervised Machine Learning," *International Journal of Artificial Intelligence and Expert Systems (IJAE)*, vol. 10, no. 2, pp. 18-25, 2022.

[14] Qasem Abu Al-Haija and Saleh Zein-Sabatto, "An Efficient Deep-Learning-Based Detection and Classification System for Cyber-Attacks in IoT Communication Networks," *Electronics*, vol. 9, pp. 2152, 2023.

[15] Hasan Alkahtani and Theyazn H. H. Aldhyani, "Intrusion Detection System to Advance Internet of Things Infrastructure-Based Deep Learning Algorithms," *Volume 2021*, Article ID 5579851, pp. 1-18, 2024.