ANOMALY DETECTION IN IOT NETWORKS WITH DEEP LEARNING ALGORITHMS

Vidhi Saxena[i]
Indira Gandhi Delhi Technical University for Women
Delhi, India
vidhi094btmae23@igdtuw.ac.in

Advika Singhal[ii]
Indira Gandhi Delhi Technical University for Women
Delhi, India
advika006bteceai23@igdtuw.ac.in

Abstract- **The rapid expansion of IoT devices in every field has brought a much-needed change in connectivity across networks. It has consequently exposed them to the most vulnerable range of cybersecurity threats. This paper proposes a hybrid deep-learning model based on the trend of combining Convolutional Neural Networks with Recurrent Neural Networks, aimed to more effectively detect cyber threats through IoT networks and now leveraging the respective strengths of CNNs in extracting spatial features and RNNs in processing complex temporal sequences. Theoretical analysis suggests that this hybrid models might outperform some of the conventional machine learning techniques, such as Logistic Regression, Naive Bayes, and Random Forest, in terms of precision, recall, accuracy, and F1-score. Additionally, incorporating Autoencoders and GANs that may be included at unsupervised levels of learning can enhance adaptability to ever-changing threats. While the model is still empirically unvalidated, interestingly enough, one would see whether the model could successfully execute real-time anomaly detection at scale while being adversarial resistant against promising approach for securing IoT networks.**

Keywords— Internet of Things, cybersecurity, deep learning, Convolution Neural Network, Recurrent Neural Network, IoT security, machine learning

I. INTRODUCTION

Coined by Kevin Ashton in 1999, the Internet of Things (IoT) refers to a network of physical objects embedded with electronics, software, sensors, and connectivity to enable communication and interaction. More than 9 billion "things" connected to the internet, a number that is growing to reach 20 billion soon. IoT devices have increased from 15.41 billion in 2015 to over 35.8 billion in 2021, transforming manufacturing, healthcare, and logistics.

The growth of IoT comes with huge security challenges. IoT malware attacks have risen with a 107% increase in the first half of 2024 alone. Devices under attack Spent an average of 52.8 hours compromised. Vulnerabilities such as CVE-2023-1389 that affected 21% small-to medium-sized businesses, highlight the severity of these threats. The absence of uniform security protocols as a result of This complexity and diversity of IoT ecosystems aggravate the issue.

Anomalies in IoT networks are usually abnormally data points or patterns that deviate from expected behaviour. Detecting these anomalies is crucial for identifying potential security threats. Existing methods for IoT anomaly detection can be classified based on their approach, application, method type, and algorithm latency. Researchers are employing artificial Intelligence and machine/deep learning to boost these processes. Out of the Deep learning models, Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory networks (LSTMs) and Autoencoders, are increasingly being used for anomaly detection in IoT networks. These models detect anomalies in the vast IoT data and the researchers compare them to find the most effective ones.

Adopting ultra-lightweight security protocols is a significant development in IoT security, which is constantly evolving to address new risks. Anomaly detection using deep learning focuses on the advancement in security of IoT networks by evaluation in real time of likely threats. It promises to increase the reliability and safety of IoT systems. But as their presence in various sectors continues to grow. That in a cybersecurity framework, for Cyber-Physical systems such as this With IoT Networks, advanced anomaly detection is required. Systems have thereby become relevantly important with the complexity and volume of network traffic and system logs.

II. LITERATURE REVIEW

The rise in each field poses major challenges in combating cyber-attacks as the Internet of Things (IoT) networks begin to complicate and become localized. Security features have turned out mostly limited in most cases, and the nature of data it has to process has made IoT a fantastic target for cyber hackers. Traditionally designed cybersecurity cannot cope up with the dynamic and heterogeneous nature of IoT networks. To cope with this challenge, many researchers have ventured into Machine learning and Deep learning to enhance threat detection and response capabilities in IoT systems A novel DCNN-based deep learning model and feature engineering method for malicious attacks in IoT networks. The goal is to increase efficiency and reduce computing power.[1] Anomaly detection algorithms are divided into four categories, which are briefly discussed in this review. It also lists the most important words and applications, and identifies the application areas that need further research. [2] Intrusion detection system based on CNN and LSTM deep learning algorithms. In the model, we group CNN and LSTM layers, and utilize the ability of CNN to extract spatial features and the ability of LSTM to extract physical features.[3] Cyber Sentinel" explores the multifaceted applications of AI and ML in cyber threat detection, encompassing anomaly detection, behavioral analysis, threat intelligence, and automated incident response.[4] It provides an overview of the current state of AI and machine learning in cybersecurity, discussing key technologies, applications, challenges, and future directions. We examine ML algorithms for tasks such as malware detection, malware classification, and network intrusion detection.[5] An overview of vulnerabilities and the current

state of IoT-related security concepts. Classify and analyze security issues found in IoT layer architectures, and lay the foundation for IoT security by analyzing existing attacks, threats, and resolution issues. [6] This study evaluates IDS performance and traffic in an IoT environment using various machine learning algorithms.[7] Convolutional neural network models are used to build different types of classification models. The proposed model is then implemented using 1D, 2D, and 3D convolutional neural networks. Transfer learning is used to achieve binary and multi-class classification using convolutional neural network multi-class pre-trained models. [8] The AI revolution in cybersecurity has begun. Through continuous research, responsible management, and ethical use, we can harness the full potential of AI to move us toward a safer, more secure digital future. [11] As the complexity and scale of cyber threats continue to increase, organizations need to be proactive and use AI and machine learning to strengthen their cyber defenses. [12] These findings not only tell us about the current requirements of AI-ML in the field of cyber-physical security but also the significant steps taken in the direction of the same. This study aims to address the gaps by proposing a novel CNN-RNN hybrid model, building on the strengths identified in existing research.

III. Proposed Methodology

In this work, we propose a hybrid model that combines Deep Learning Algorithms - Convolutional Neural Networks (CNNs), and Recurrent Neural Networks (RNNs). This model offers a robust approach to tackle these challenges. CNNs are known to extract spatial features from data and thus appropriate for analyzing patterns within network traffic that can be portrayed as images or sequences of spatial data. RNNs, especially by means of Long Short-Term Memory (LSTM) or Gated Recurrent Unit (GRU) cells, which can process sequential data memorizing information and are, thus, very well-suited for the tasks of analyzing the temporal aspects of network traffic.

When the output from the CNN layers is passed to the RNN layers, the model captures both, spatial and temporal patterns in the data. Therefore, the hybrid model integrates the capability of the CNNs and RNNs, setting scope for further comprehensive analysis of network behavior.

To make the model extend so that it picks anomalies significantly, especially in cases where there are no labeled data, Autoencoders and Generative Adversarial Networks (GANs) could be added to the training. Autoencoders are a type of neural network designed to learn efficiently in an unsupervised way the data representation. Then the latent space representation can be passed into the CNN-RNN hybrid model to enrich the feature set for anomaly detection.

GANs are particularly useful for generating synthetic data, which can be instrumental in training the model under conditions where the real-world data on attacks is limited. This adversarial process provides a diverse set of data for training the CNN-RNN model and helps improve its robustness by exposing it to a wide range of potential threats.

A hybrid model is appropriate for large and complex IoT networks considering scalability, efficiency, and robustness against adversarial attacks, and the specific model used is apt for the research purpose. Scalability horizontally will allow distributed processing and the system will then easily handle large volumes of traffic. It designs the architecture of its model very carefully and optimizes computational resources to make its model execution more efficient. The adversarial training approach allows this model to learn from the examples trying to manipulate its output. Thus, it gains a greater sense of resilience by learning about the tampered inputs and handles them suitably.

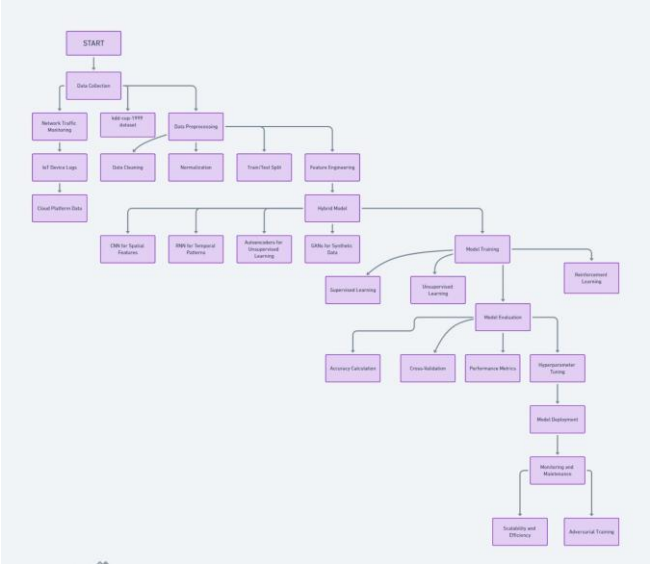

Fig.2 Visualization of the proposed framework with stages and connections.

A. *Model Training*

The hybrid model can be trained by using variety of strategies with respect to labeled data and the demands of the application at hand. This approach is based on the cumulative use of supervised, unsupervised, and reinforcement learning that would combine both known and emerging threats in the IoT environment in breadth.

a. For supervised training, the model is trained on a labeled dataset, and each input is assigned a known output of, say, normal or anomalous traffic. This approach is highly effective when a large and diverse labeled dataset is equipped, as it allows the model to learn explicit mappings from inputs to outputs.

b. Unsupervised training does not rely on labeled data. Instead, techniques like Autoencoders or GANs are utilized to model the underlying distribution of the data. These methods are useful for anomaly detection, where the model learns to identify outliers that deviate from the learned distribution of normal traffic.

c. Reinforcement learning offers another approach, particularly suitable for dynamic environments like

IoT networks where threats evolve. The reward function is designed to incentivize behaviors that enhance security, such as reducing the number of successful attacks or minimizing false positives. Through exploration and exploitation, the agent gradually learns the most effective strategies for maintaining network security.

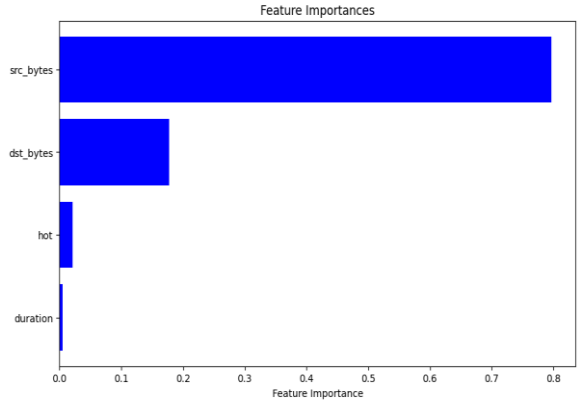

Fig.2 Feature Importance of different datasets

B. *Data Collection*

a. Network Traffic Monitoring involves capturing and investigating network packets transmitted across IoT networks. Data is collected from IoT gateways, edge devices, and network routers/switches using tools like Wireshark.

b. Logs generated by IoT devices, including access attempts, errors, and configuration changes, can be collected and analyzed. Logs are sourced from IoT devices such as sensors, smart appliances, and cameras.

c. Data from IoT devices connected to cloud platforms can be accessed through APIs and log aggregation services. Data is collected from Microsoft Azure IoT, and Google Cloud IoT, providing a wide range of device interactions and performance metrics.

d. Pre-existing datasets that contain labeled instances of normal and malicious activities are used to train the model. Publicly available datasets like NSL-KDD, UNSW-NB15, and IoT-23 can be utilized along with custom simulations, conducted to generate synthetic datasets that replicate real-world IoT environments. We will use this method for the purpose of this research.

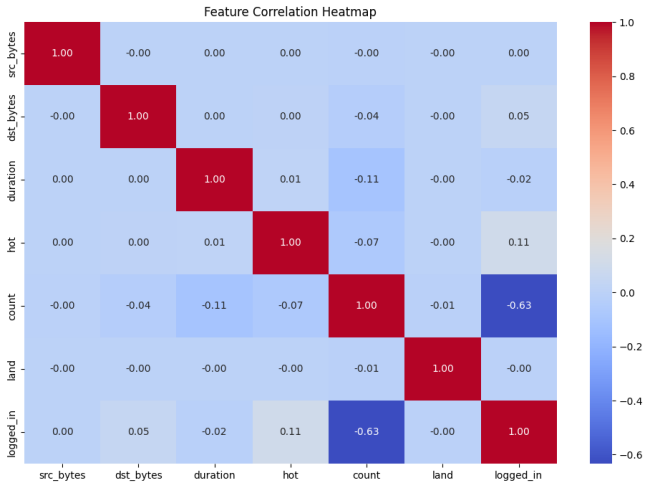

Fig.3 Feature Correlation Heat Map

C. *Limitations and Potential Biases*

Despite the strengths of the proposed methodology, several limitations and potential biases should be acknowledged.

a. Data limitations include biases towards certain devices or networks or insufficient complexity and variability of actual IoT environments in synthetic data, which can lead to an increased rate of false results in real-world deployments.

b. Real-time processing demands might lead to increased latency, impacting the model's ability to detect and respond to threats promptly.

c. The reliance on human-defined labels for supervised learning introduces the potential for bias and can result in a model that is overly tuned to specific types of threats.

IV. Result And Discussion

We developed a model using logistic regression, Naive Bayes, and Random Forest to theoretically interpret the results obtained if the proposed hybrid CNN-RNN model for cybersecurity in IoT networks is fully implemented. The discussion focuses on the expected performance and potential improvements over traditional models based on theoretical considerations and a current understanding of deep learning models in the context of IoT security.

A. *Expected Confusion Matrix*

1. Confusion Matrix Components:

a. True Positives (TP): Number of correct predictions for the positive class.

b. True Negatives (TN): Number of correct predictions for the negative class.

c. False Positives (FP): Number of incorrect predictions where the model incorrectly predicted the positive class.

d. False Negatives (FN): Number of incorrect predictions where the model incorrectly predicted the negative class.

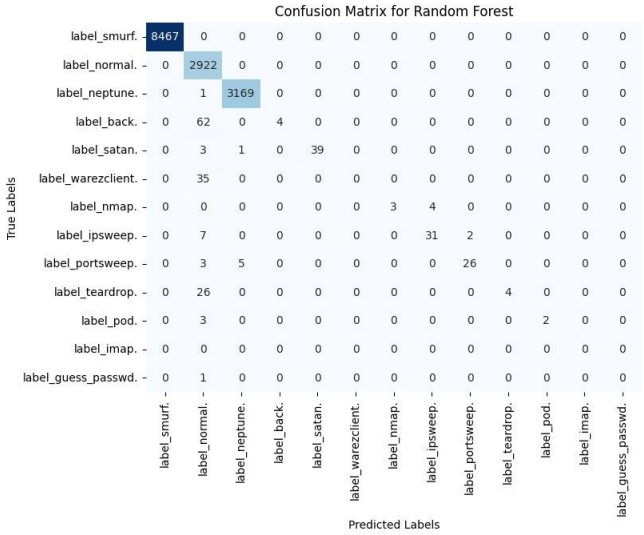

Fig. 4 Confusion Matrix for Random Forest

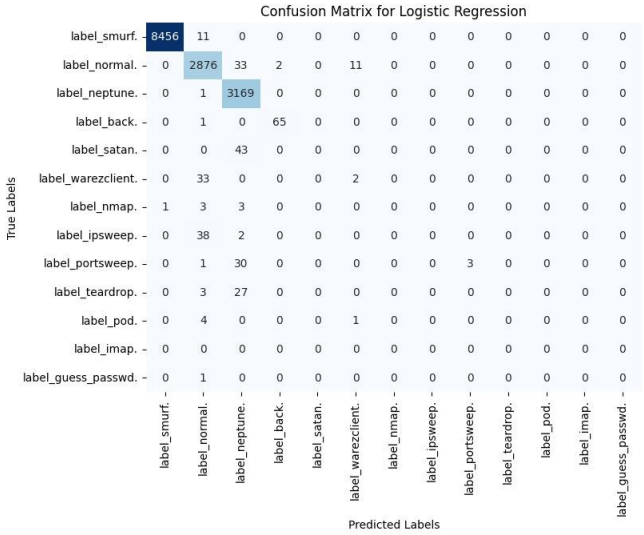

Fig. 5 Confusion Matrix for Logistic Regression

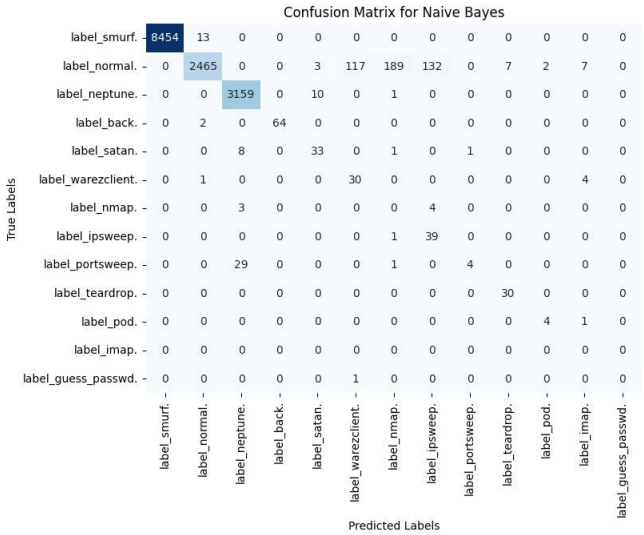

Fig. 5 Confusion Matrix for Naïve Bayes

For the hybrid CNN-RNN model, the confusion matrix is anticipated to show significant improvements in detecting true positives (TP) while minimizing false positives (FP) and false negatives (FN) compared to traditional models. The theoretical breakdown can be studied through Table I where we have taken mean to calculate the expected values for Hybrid CNN-RNN Model.

2. Discussion:

The hybrid CNN-RNN model is expected to perform better in distinguishing between normal and malicious activities due to its ability to learn hierarchical representations of data. Given the confusion matrix components (TP, FP, TN, FN) from a basic model, the expected improvements of a CNN-RNN Model can be understood by:

a. Expected True Positives (TP') & Expected True Negatives (TN'):

$$TP' = TP \times (1 + \Delta TP)$$
$$TN' = TN \times (1 + \Delta TN)$$

Where ΔTP and ΔTN are the expected improvement in true positives and negatives due to the CNN-RNN model's superior features.

b. Expected False Positives (FP') & Expected False Negatives (FN'):

$$FP' = FP \times (1 - \Delta FP)$$
$$FN' = FN \times (1 - \Delta FN)$$

Where ΔFP and ΔFN are the expected percentage decrease in false positives and negatives.

The CNN component would efficiently capture spatial features within network traffic data, while the RNN would handle temporal dependencies, leading to higher TP and TN values.

B. Performance Metrics by Model

1. Table II illustrates the hypothetical performance metrics of the proposed hybrid model in comparison to the existing models using weighted average approach.

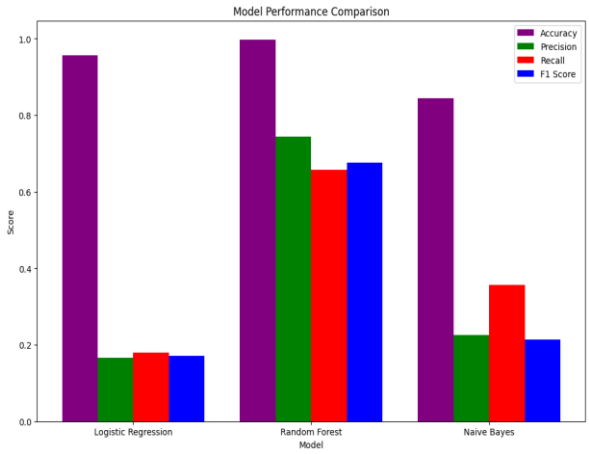

Fig. 6 Model Performance Comparision between Logistic Regression, Random Forest and Naïve Bayes.

2. Discussion: The expected performance test shows that the hybrid CNN-RNN model will improve accuracy, precision, recall, and F1-score compared to traditional models. Using the adjusted confusion matrix components, you can then calculate the expected performance metrics as follows:

   a. **Expected Accuracy**:
   Accuracy'= (TP′+TN′) ÷ (FP′+FN+′TP′+TN′)

   b. **Expected Precision**:
   Precision'=TP′ ÷ (FP′+TP′)

   c. **Expected Recall**:
   Recall'=TP′ ÷ (FN′+TP′)

   d. **Expected F1-Score**:
   F1-Score'=2 × ((Precision'× Recall') ÷ (Precision'+ Recall'))

Deep Learning The deep learning architecture, with its ability to capture both spatial and temporal aspects of network traffic, is likely to result in more robust detection capabilities. Traditional models might miss complex patterns or exhibit bias in certain types of traffic, leading to lower performance metrics overall.

C. Training Time of the Model

1. Training time is a crucial factor, particularly in resource-constrained IoT environments. The expected training times for the proposed hybrid model compared to traditional models can be studied through Table III using weighted average.

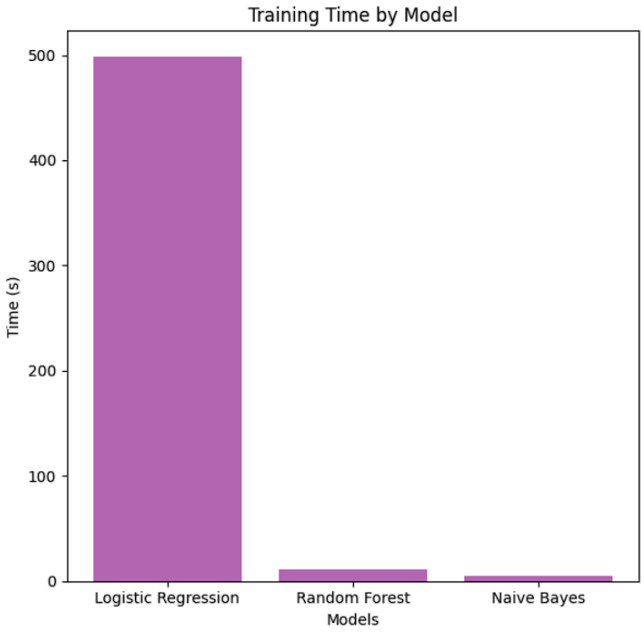

Fig. 7 Comparison of Training Time taken by traditional models.

2. Discussion:
The proposed hybrid model is expected to require significantly more training time compared to traditional models due to its complexity which can be understood by,

Training Time`=

Training Time (basic model)×(1+Δtime)

Where Δtime reflects the additional time required due to the added layers and parameters in the deep learning architecture, involving both CNNs and RNNs, would necessitate more computational resources and time for training, especially as it processes large and complex datasets. Traditional models, while quicker to train, might not offer the same level of accuracy or resilience against advanced threats.

TABLE I
EXPECTED CONFUSION MATRIX VALUES FOR PROPOSED MODEL

Models	True Positives (TP)	False Positives (FP)	True Negatives (TN)	False Negatives (FN)
Naive Bayes	13836	599	31689	152
Random Forest	14106	607	31675	127
Logistic Regression	14096	673	31664	191
Hybrid CNN-RNN (Expected)	14013	626	31676	157

(Source: Authors compilation))

TABLE II
EXPECTED MODEL PERFORMANCE VALUES FOR PROPOSED MODEL

Metric	Logistic Regression	Naive Bayes	Random Forest	Hybrid CNN-RNN (Expected)
Accuracy	0.9561	0.9972	0.8438	0.9328
Precision	0.1666	0.7384	0.2253	0.3907
Recall	0.1799	0.6569	0.3557	0.4140
F1-Score	0.1707	0.6730	0.2141	0.3668

(Source: Authors compilation)

TABLE III
EXPECTED TRAINING TIME TAKEN BY HYBRID MODELS.

Model	Logistic Regression	Naive Bayes	Random Forest	Hybrid CNN-RNN (Expected)
Training Time (Hours)	498.14	10.93	4.67	302.63

(Source: Authors compilation)

D. Assumptions

1. ΔTP, ΔFP, ΔTN, ΔFN are theoretical improvement factors based on the deep learning model's anticipated ability to capture complex patterns in the data.
2. These factors could be estimated based on empirical improvements seen in similar tasks or by conducting a small-scale preliminary experiment

V. CONCLUSION

This study presents a hybrid model concept that combines Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) to enhance the cybersecurity of IoT networks. The model is designed to leverage the strengths of both CNNs and RNNs for improved detection accuracy and adaptability to evolving threats. Theoretical analysis suggests that the hybrid model could outperform traditional machine learning methods in key performance metrics. While the model remains theoretical, it provides a strong foundation for future research and practical implementation, aiming to offer a scalable, robust, and real-time solution for securing IoT environments.

REFERENCES

[1] Ullah, Safi & Ahmad, Jawad & Khattak, Muazzam & Alkhammash, Eman & Hadjouni, Myriam & Ghadi, Yazeed & Saeed, Faisal & Pitropakis, Nikolaos. (2022). A New Intrusion Detection System for the Internet of Things via Deep Convolutional Neural Network and Feature Engineering. Sensors. 22. 3607. 10.3390/s22103607.

[2] Ayan Chatterjee, Bestoun S. Ahmed, IoT anomaly detection methods and applications: A survey, Internet of Things, Volume 19, 2022, 100568,ISSN 2542-6605, https://doi.org/10.1016/j.iot.2022.100568.

[3] Ha, Asmaa & Gunawan, Teddy & Habaebi, Mohamed & Halbouni, Murad & Kartiwi, Mira & Ahmad, Robiah. (2022). CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System. IEEE Access. PP. 1-1. 10.1109/ACCESS.2022.3206425. https://www.ibef.org/industry/msme-presentation accessed on 30 August 2023.

[4] (2023). Cyber Sentinel: Leveraging AI and ML for Advanced Threat Detection.

[5] Katiyar, Dr & Tripathi, Mr & Kumar, Mr & Verma, Mr & Sahu, Dr & Saxena, Dr. (2024). AI and Cyber-Security: Enhancing threat detection and response with machine learning.. Educational Administration Theory and Practices. 30. 10.53555/kuey.v30i4.2377.

[6] Tariq U, Ahmed I, Bashir AK, Shaukat K. A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. Sensors. 2023; 23(8):4117. https://doi.org/10.3390/s23084117L.

[7] Fahad Ali Alotaibi , Shailendra Mishra Cyber Security Intrusion Detection and Bot Data Collection using Deep Learning in the IoT (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 15, No. 3, 2024

[8] IMTIAZ ULLAH AND QUSAY H. MAHMOUD , Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks and July 30, 2021. Doi: 10.1109/ACCESS.2021.3094024

[9] Ahsan Nazir, Jingsha He, Nafei Zhu, Saima Siraj Qureshi, Siraj Uddin Qureshi, Faheem Ullah, Ahsan Wajahat, Muhammad Salman Pathan, A deep learning-based novel hybrid CNN-LSTM architecture for efficient detection of threats in the IoT ecosystem, Ain Shams Engineering Journal, Volume 15, Issue 7, 2024, 102777, ISSN 2090-4479, https://doi.org/10.1016/j.asej.2024.102777.

[10] https://blog.checkpoint.com/security/check-point-research-cyber-attacks-increased-50-year-over-year/

[11] Ashok Manoharan, Mithun Sarker, REVOLUTIONIZING CYBERSECURITY: UNLEASHING THE POWER OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING FOR NEXT GENERATION THREAT DETECTION Volume:04/Issue:12//December -2022 doi: https://www.doi.org/10.56726/IRJMETS32644

[12] (2024). Unleashing the Cyber Titans: How AI and ML Are Shaping Future Threat Detection AUTHORS:IBRAHIM A.