International Journal of Emerging Research in Engineering and Technology
Pearl Blue Research Group| Volume 2, Issue 1, 27-36, 2021
ISSN: 3050-922X | https://doi.org/10.63282/3050-922X.IJERET-V2I1P104

Original Article

Enhancing IoT (Internet of Things) Security Through Intelligent Intrusion Detection Using ML Models

Mukund Sai Vikram Tyagadurgam[1], Venkataswamy Naidu Gangineni[2], Sriram Pabbineedi[3], Mitra Penmetsa[4], Jayakeshav Reddy Bhumireddy[5], Rajiv Chalasani[6]
[1]University of Illinois at Springfield.
[2]University of Madras, Chennai.
[3]University of Central Missouri.
[4]University of Illinois at Springfield.
[5]University of Houston.
[6]Sacred Heart University.

Abstract - *Through IoT technology wireless communications experience a fundamental transformation that reshapes various industries. Multiple cyberattacks exploit the limited capacity and broad exposure among IoT networks. IDS systems require advanced technologies because existing security systems fail to detect new potential threats. This research proposes Long Short-Term Memory (LSTM)-based deep learning models to develop an intelligent intrusion detection system (IDS) that improves IoT security. The LSTM model performs training on the ToN-IoT dataset data after applying multiple preparation steps, including cleaning and normalization and encoding different features. The model's remarkable detection skills are demonstrated by a number of evaluations, such as its 99.41% detection accuracy, 99.35% precision, 99.32% recall, and 99.33% F1-score. By employing an implemented LSTM model researcher could achieve higher classification success rates than a DBN model serves as validation for monitoring threat detection and temporal pattern measurement. The suggested method provides a strong, scalable, and flexible IoT intrusion detection solution, enhancing security for IoT settings that are becoming more intricate and networked.*

Keywords - *Industrial Internet of Things (IOT), Smart Industry, Big Data Analytics, Real-time Monitoring, Digital Transformation.*

1. Introduction

The IoT established its name in 1999 then evolved into an essential wireless communication paradigm. The field of ICT has made IoT a top research priority that receives intense interest from both academia and the industry [1]. A network is the fundamental building block of the IoT that connects embedded computers with smart sensors and RFID tags along with automated devices and IoT gateways and remote servers. Physical devices using local networks and the worldwide Internet can connect to services and devices for data sharing [1]. The IoT now directs a technological revolution through dozens of sectors, spanning automotive networks as well as supply chains and retail stores, combined with healthcare facilities and smart residential developments. The increasing number of IoT networks has turned security and privacy issues into critical problems [2]. Intelligent environments may be at risk due to the security flaws in IoT-based technologies, making IDS essential to mitigate attacks that exploit these vulnerabilities.

All security protocols struggle to understand and counter the widespread vulnerabilities of IoT networks from device interconnections across multiple devices [3]. The limited resources of IoT systems prevent the direct implementation of security procedures that succeed in traditional systems. Specialized IDSs for IoT environments have become more sought after due to this growing need [4]. Most research on IoT intrusion detection centers on rule-based detection methods that excel at known attacks but prove ineffective against new and zero-day threats. Anomaly-based detection methods have emerged as practical solutions to monitor the quick IoT ecosystem growth as well as continuous data flows from various linked devices [5][6]. These methods are especially important for detecting previously unknown threats in real time, where traditional rule-based systems fall short.

Security for IoT devices improves through creative approaches enabled by machine learning-based IDS. Analysis of device monitoring and network activity through ML-based information patterns indicates potential threats. These models show excellent suitability in IoT environments because they handle big quantities of data beyond human potential analysis [7][8]. Platform attacks become detectable through ML methods which also maintain the capability to adapt their detection to new cyberthreat patterns. Real-time threat detection using ML-based systems enables prompt application of suitable mitigation techniques and reactions [9][10]. The use of ML has great promise for IoT security, particularly in emerging network infrastructures such as 5G, where network slicing and complex communication patterns require advanced security measures.

Intrusion detection systems that utilize ML have undeniable promise in IoT settings, there remains a lack of comprehensive, methodical research addressing key challenges such as scalability, performance optimization, and real-time processing [11][12]. This study investigates how to increase the safety of IoT networks by combining anomaly-based intrusion detection systems with ML techniques. Tests of these systems' real-time attack detection capabilities for both known and unexpected threats [13], Improving defenses mechanisms and furthering the area of IoT security are the goals of this project capable of securing increasingly complex and interconnected environments.

1.1. Motivation and Contribution of Study.

In reaction to the development of connected devices, which makes IoT networks vulnerable to a wide spectrum of cyber-attacks, the IoT has become an increasingly important part of modern life. Unfortunately, real-time detection of complex and ever-changing threats is frequently beyond the capabilities of traditional security systems. This work aims to improve IoT security by protecting sensitive data and effectively identifying malicious actions using DL, more especially LSTM networks. Finding a better, more scalable, and adaptable way to secure IoT environments where accurate and rapid threat detection is paramount is the goal of this study. What follows is a list of what the study contributed:

- **Development of an LSTM-based Model:** The paper introduces an LSTM DL model trained specifically to identify assaults in IoT settings by capitalizing on its capacity to record trends in network traffic over time.
- **Comprehensive Data Pre-processing:** A robust data pre-processing pipeline is implemented, including data cleaning, normalization using min-max scaling, and categorical feature encoding, ensuring that the ToN-IoT dataset is accessible for model training.
- **Evaluation Using Standard Metrics:** The model's performance is rigorously examined using a number of standard classification criteria, including accuracy, precision, recall, F1-score, and ROC curve analysis, ensuring a comprehensive evaluation of its detection capabilities.
- **Demonstration of Effectiveness:** The experimental results validated the model's promise for practical use in IoT security, as demonstrated by its ability to distinguish between benign and harmful activities in IoT networks.

1.2. Justification and Novelty of the Study

This study is justified by the increasing demand for strong security measures that are adapted to the particular difficulties of IoT networks, which are extremely dynamic and susceptible to a variety of cyberthreats. Utilizing a LSTM DL model, It is particularly suitable for finding temporal correlations in sequential network data a feature that typical ML models sometimes overlook is what makes the suggested method distinctive. By utilizing the ToN-IoT dataset and applying thorough pre-processing techniques, the study ensures realistic and diverse input for training, enhancing the generalizability of the concept across different IoT attack scenarios. The integration of LSTM with this comprehensive pipeline offers a more adaptive and intelligent intrusion detection solution, advancing the current state of IoT cybersecurity.

1.3. Structure of Paper

The structure of the paper is as follows: IoT intrusion detection research is reviewed in Section II. The suggested LSTM-based technique is explained in Section III. The findings and discussion are shown in Section IV. The paper's conclusion and future directions are outlined in Section V.

2. Literature Review

This section includes relevant research that focus on IoT security via intelligent intrusion detection systems. Table I presents a comprehensive summary of the extant literature, summarizing key approaches, methodologies, datasets used, and the outcomes achieved in various studies. Huong et al. (2019) suggest a revolutionary DL technique that uses a CNN to detect breaches in IoT networks retrieving location and service logs from an IoT system, resulting in a unique feature set, address, and so on. For training and detection, the initial feature set is then refined, encoded into a digital matrix, and fed into a CNN. The suggested technique has an average accuracy of 98.9% and is assessed using the cross-validation approach [14].

Roopak, Tian and Chambers (2019) recommend DL models for cybersecurity in IoT networks. One such technology that might link living and non-living objects worldwide is the Internet of Things network. DDoS assaults have impacted a number of IoT networks in recent years, resulting in large losses. Using the most recent CICIDS2017 datasets, they assessed their suggested DL models for detecting DDoS attacks, which produced the highest accuracy of 97.16% [15]. Alrashdi et al. (2019) suggest that in a smart city, IoT cybersecurity threats are addressed by an AD-IoT system, an intelligent anomaly detection system built on RF and ML algorithms. The suggested method for locating hacked IoT devices at dispersed fog nodes could work. It evaluated and demonstrated the accuracy of their model using a current dataset. According to their findings, the AD-IoT can attain the greatest classification accuracy of 99.34% and the lowest FP rate [16].

Roy and Cheung (2018) provide a new DL method that uses a BLSTM RNN to identify assaults in IoT networks. A multi-layer DLNN is trained using UNSWNB15, A fresh set of benchmark data. The binary classification of common and harmful actions on the Internet of Things network is the main topic of this study. The outcomes of the experiment demonstrate the high performance of their suggested model in terms of FAR, F1 score, accuracy, and memory. their suggested BLSTM model has a 95% accuracy rate in detecting attacks [17]. Ertam, Kilinçer and Yaman (2017) The data collection process used ML techniques to analyze if online data points were normal or abnormal. A study is performed to achieve this goal, NB, BN, RF, and MLP are used in the KDD Cup 99 data collection, and SMO classification methods used in the literature study.

The accuracy of classifiers is evaluated through numerical accuracy rates in addition to false rate metrics and precision and recall measurements and F-measure metrics. Comparison is also used to provide classifier classification times [18]. Hodo et al. (2016) research examines IoT threats while developing ANN-based security solutions. The research uses Internet packet traces to develop a multi-level perceptron ANN while evaluating its performance in identifying DDoS/DoS assaults. The study focusses on identifying common and risky practices in IoT networks. The simulation of IoT networks serves to confirm ANN operations. The testing findings show that they can successfully identify a variety of DDoS/DoS assaults with an accuracy of 99.4% [19]. This section examines the body of research on ML-based intrusion detection in IoT environments, with Table I providing an overview of the most important works.

Table 1: Summary of literature review based on IoT Intrusion Detection Using ML Models.

Author	Methodology	Data	Key Findings	Limitation	Future Work
Huong et al. (2019)	Deep learning for IoT intrusion detection using CNN	IoT log data (location, service, address)	Achieved 98.9% accuracy using cross-validation	Limited feature diversity; may not generalize well across all IoT environments	Expand feature extraction and test on diverse real-world datasets
Roopak, Tian, and Chambers (2019)	Deep learning for identifying DDoS assaults on the Internet of Things	CICIDS2017	Achieved 97.16% accuracy in detecting DDoS attacks	Focused only on DDoS; lacks evaluation for other attack types	Broaden detection to include multiple types of attacks
Alrashdi et al. (2019)	Anomaly Detection in Smart Cities using Random Forest (AD-IoT system)	Custom smart city dataset	99.34% accuracy and a low false-positive rate were attained.	May not perform as effectively on non-smart city datasets	Integrate with real-time fog/edge computing environments
Roy and Cheung (2018)	Bi-directional LSTM RNN for binary classification (normal vs attack)	UNSW-NB15	Achieved over 95% accuracy in detecting IoT network attacks	Binary classification only; does not handle multi-class scenarios	Extend the model for multi-class classification and real-time detection
Ertam, Kilinçer and Yaman (2017)	Machine learning techniques including Naive Bayes, Bayes Net, Random Forest, MLP, and SMO were used for classification.	KDD Cup 99	SMO and RF displayed higher accuracy; classifiers were examined using false rate, accuracy, precision, recall, and the F-measure.	Relied on the outdated KDD 99 dataset, which lacks recent attack patterns; did not explore ensemble models.	Future research might involve using more recent and realistic datasets and researching deep learning approaches.
Hodo et al. (2016)	A Neural Network Artificially (MLP) to identify DDoS/DoS assaults	Simulated IoT network traffic	Achieved 99.4% accuracy; effectively detects DDoS/DoS attacks	Evaluated on simulated data only	Validate on real-world IoT network traffic and expand to broader threats

3. Methodology

The proposed IoT threat detection implementation depends on an LSTM DL model as shown in Figure 1. In order to determine model compatibility, the ToN-IoT dataset first undergoes cleaning operations, normalization using min-max scaling techniques, and categorical transformation processes. Model generalization evaluation utilizes distributed processed data between training and testing subsets. When given data from the training subset, the LSTM model develops the ability to recognize temporal behavioral signatures associated with various cyber-attack types. The model's performance is assessed using common classification measures such as accuracy, precision, recall, F1-score, and ROC curve analysis after it has been trained on unknown data. According to the

results, the model can successfully differentiate between harmful and benign network activities in Internet of Things contexts. The suggested methodology's flow diagram is shown in Figure 1.

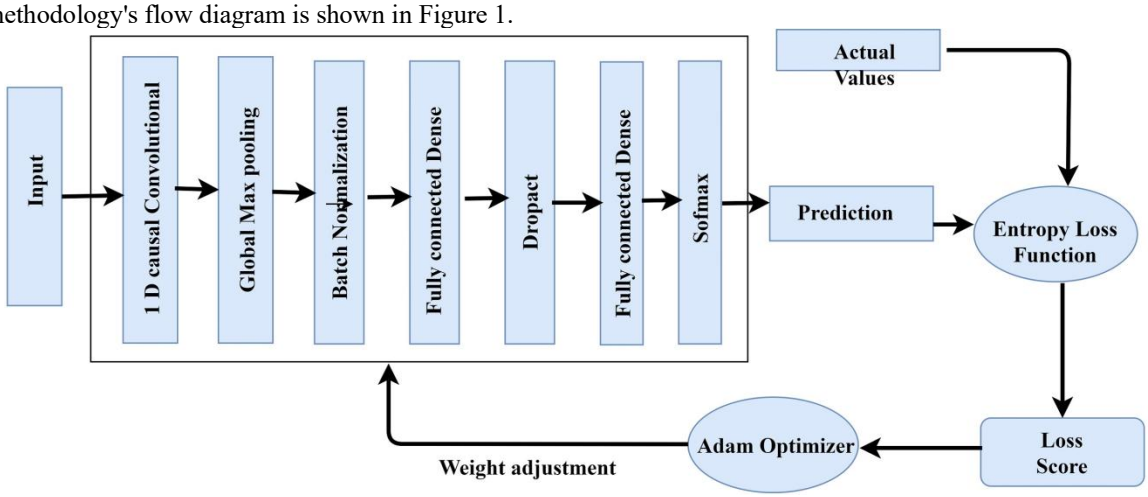

Fig 1: Flowchart of the proposed LSTM-based Internet of Things.

The following sections provide each step description that also shows in methodology and proposed flowchart:

3.1. Data Collection (ToN-IoT Dataset)

In 2019, the ACCS released the ToN-IoT dataset, designed specifically for evaluating cybersecurity solutions in IoT environments. The dataset captures network traffic generated within an IoT ecosystem, with a significant portion comprising malicious activities. It includes a total of 22,339,021 samples, of which 796,380 are benign (normal) and 21,542,641 represent various types of attacks. The dataset features 44 unique attributes extracted using the Bro-IDS (now Zeek) tool. IoT includes a wide variety of cyberthreats, including as injection attacks, ransomware, DoS, MITM, and XSS, brute-force password attempts, and network scanning.

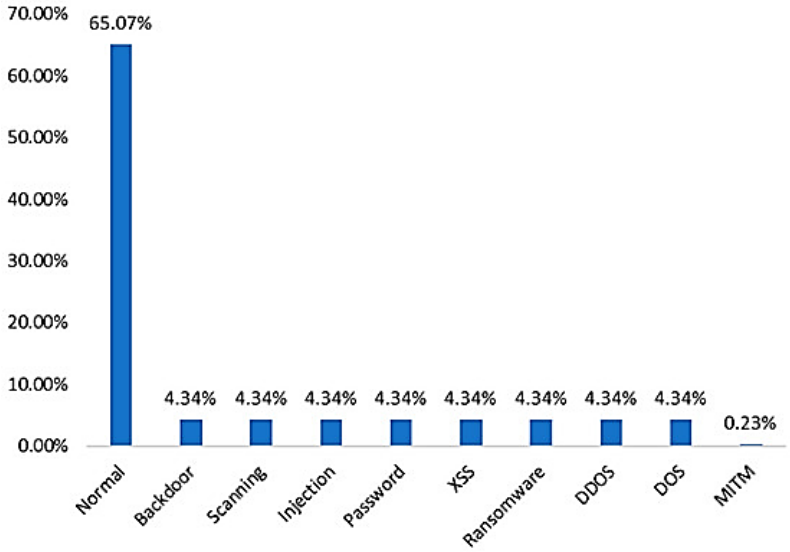

Fig 2: Data Distribution of the ToN-IoT Dataset.

The ToN-IoT dataset's data distribution is shown in Figure 2, which also shows a notable class imbalance. The majority of the data, 65.07%, is labelled as "Normal," while each attack type including Backdoor, Scanning, Injection, Password, XSS, Ransomware, DDoS, and DoS accounts for 4.34% of the data. The MITM category has the smallest representation, comprising only 0.23% of the dataset. This distribution emphasizes the prevalence of normal traffic and the underrepresentation of certain attack types, posing challenges for building balanced and efficient models for intrusion detection.

3.2. Data Preprocessing

In the examination of ToN-IoT datasets, preprocessing is crucial since raw data might contain anomalies, incomplete flows, and missing or duplicated information. In order to facilitate the development and training of a model with improved performance and fewer mistakes, it aims to provide a cleaner dataset. As stated below, it involves a number of procedures, such as feature encoding, data normalization, and data purification.

3.2.1. Data Cleaning

Data cleansing involves handling missing, inconsistent, or duplicated entries. This step ensures the integrity and quality of the dataset. The ToN-IoT dataset's logs include null values, duplicate flows, or incorrectly formed timestamps that need to be fixed.

3.2.2. Data Normalization (Min-Max Scaling)

In order to scale numerical characteristics to a standard range and prevent any one feature from dominating because of its scale, normalization is necessary. In ToN-IoT, features like packet size, duration, and number of bytes transferred can have widely different ranges. Additionally, because the dataset contains several characteristics with values on different scales, it must be normalised. Feature scaling is achieved through the use of Min-Max Scaling normalization.
This approach scales every feature in their dataset from 0 to 1. Min-Max Scaling Equation (1):

$$x'_i = (x_i - x_{min}) * \frac{b - a}{(x_{max} - x_{min})} + a$$

This formula uses x_i as the original value and x_{min} and x_{max} as the feature's minimum and maximum values inside the dataset and a and b define the desired scaling range. The output x'_i is the normalized value. This technique is extremely helpful in ML to make sure that features contribute evenly to the model, particularly for algorithms that rely on distance or when the sizes of the input data differ.

3.2.3. Feature Encoding

The process of transforming categorical variables into numerical values for processing by ML algorithms, which work with numbers, is known as feature encoding. The ToN-IoT dataset includes features such as device type, protocol names, and log types that need to be encoded. Label Encoder was used for feature encoding. Each category formula is given a distinct number by label encoding Equation (2):

$$x_{encoded} = LabelEncoder(x)$$

The formula $x_{encoded} = LabelEncoder(x)$ denotes the conversion of categorical data into numeric form by assigning each unique category in x a distinct integer value using label encoding.

3.3. Data Splitting

This method divides the entire dataset into two groups. The remaining 20% of the data is used to test the model after it has been trained on 80% of it.

3.4. Proposed LSTM Model

Long-term dependencies might be remembered because to LSTM, which was initially suggested for language models in 1997. The LSTM layers are made up of memory blocks with three multiplicative gates in each that are connected recurrently. For a certain amount of time, gates continuously write, read, and reset data to guarantee that the temporary data is used.

Unlike from traditional recurrent unit, LSTM unit keeps the current memory$c_t, \in \mathbb{R}^n$. The input of the unit,x_t, h_{t-1}, c_{t-1} and the output of the unit,$h_t, c_t$are updated as follows in Equation (3-8):

Gates:

$$i_t = \sigma(W_i x_t + U_i h_{t-1} + b_i$$
$$f_t = \sigma(W_i x_t + U_f h_{t-1} + b_f$$
$$o_t = \sigma(W_o x_t + U_o h_{t-1} + b_o$$

Input Transform:

$$g_t = tanh(W_g x_t + U_g h_{t-1} + b_g$$

State Update:

$$c_t = f_t \odot c_{t-1} + i_t \odot g_t$$

$$h_t = o_t \odot tamh(c_t)$$

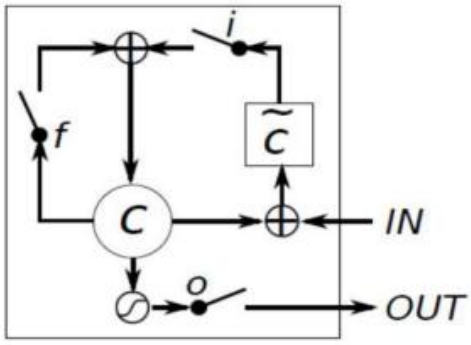

Fig 3: LSTM Single Cell Structure

The logistic sigmoid function with multiplication by elements are represented by the symbols σ and $\odot$, respectively, in the equations above in Figure 3. The LSTM unit has an input gate i_t, a forget gate f_t, an output gate o_t, a hidden unit htt and a memory cell c_t at each time step t. The learnt parameters are W and U, and the additional bias is indicated by b. It makes sense that the input gate regulates the amount of updating of each unit, the forget gate regulates the amount of erasing of the memory cell, and the output gate regulates the amount of internal memory state that is exposed.

3.5. Performance Matrix

The efficacy of the suggested intrusion detection models for IoT security to differentiate between benign and malevolent network traffic was evaluated using conventional performance measures. A confusion matrix was applied to compare predicted and actual labels, offering insights into precision, recall, and overall accuracy. These metrics were obtained from TP, TN, FP, and FN, where FP and FN denote occurrences of misclassified traffic while TP and TN represent correctly recognised traffic.

Accuracy: The system's capacity to classify attack packets as either attack or regular. Forecasts of any proportion are permissible for all samples. Equation (9) provides a mathematical expression for accuracy:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Precision: defines the proportion of actual assaults found compared to all packets marked as attacks; it is calculated arithmetically in Equation (10).

$$\text{Precision} = \text{TP} / \text{TP} + \text{FP}$$

Recall: The capacity of the system to accurately identify assaults when a security breach occurs is sometimes referred to as the TP rate, and it may be mathematically stated as follows in Equation (11):

$$\text{Recall} = \text{TP} / \text{TP} + \text{FN}$$

F1-Score: In theory, F1 represents the harmonic mean of accuracy and recall. Equation (12) gives a numerical representation of it:

$$F1 = 2 * \frac{(Precision * Recall)}{(Precision + Recall)}$$

ROC: The trade-off at various thresholds between TPR and FPR settings is depicted graphically by the ROC curve, which shows how well a binary classification model performs. AUC, or the model's capacity to distinguish between classes is gauged by the area under the ROC curve; a number nearer 1 denotes superior performance.

4. Results And Discussion

The section on experimental setup, performance evaluation metrics, testing outcomes, and the results of this section offers a thorough rundown of IoT intrusion detection using the ToN-IoT dataset. An NVIDIA GTX 960 graphics card, an Intel I5 6300HQ4 CPU, 12 GB of RAM, and the Python programming language were all installed on a Windows 10 computer for the simulation testing. The experiment results of the proposed LSTM model are provided in Table II. The LSTM model's performance, reaching high levels of the ToN-IoT dataset, produces exceptional and well-balanced classification results, including accuracy (99.41%), precision (99.35%), recall (99.32%), and F1-score (99.33%).

Table 1: Results of Proposed Model (LSTM)

Matrix	LSTM
Accuracy	99.41
Precision	99.35
Recall	99.32
F1 score	99.33

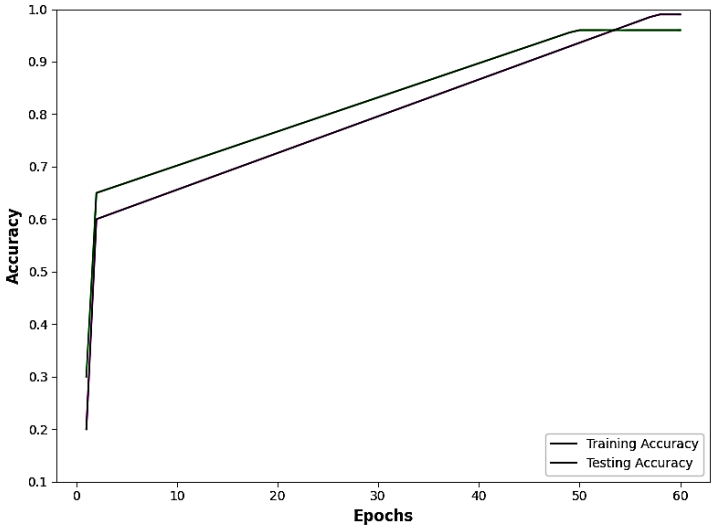

Fig 4: Accuracy Curve for LSTM

Figure 4 illustrates the accuracy of an ML model's training and testing throughout 60 epochs, where epochs are plotted on the x-axis, whereas the y-axis shows accuracy. A purple line reflects training accuracy, whereas testing accuracy is depicted in green. The accuracy of both curves increases sharply in the first few epochs before steadily improving to around 0.99 for training and 0.96 for testing, indicating successful learning and generalization. The close alignment of both curves suggests minimal overfitting and effective model performance across the dataset.

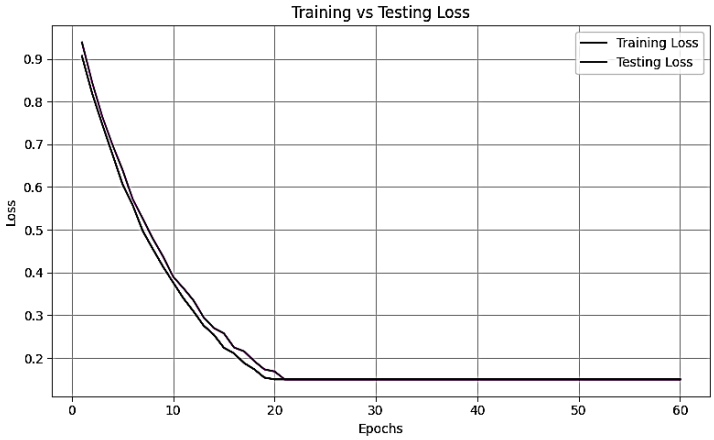

Fig 5.: Loss Curve for LSTM

The Figure 5 illustrates the comparison between training and testing loss over 60 epochs for a ML model. The training and testing loss curves both show a steady decrease, suggesting that learning was successful in the first 20 epochs. Both losses plateau and stay almost consistent after around epoch 20, indicating that the model has converged and that performance is not greatly enhanced by additional training. The close alignment of the two curves implies good generalization, with no significant overfitting observed during the training process.

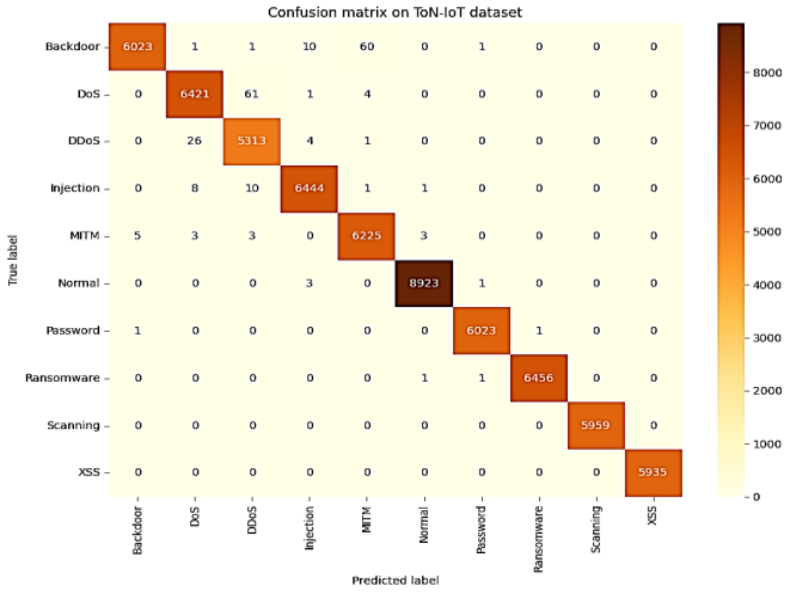

Fig 6: Confusion Matrix for LSTM

A confusion matrix assessing the effectiveness of a classification model on the ToN-IoT dataset, which includes 10 types of network traffic, is shown in Figure 6, encompassing both typical activity and different kinds of cyberattacks. The number of times the projected class (columns) matched or deviated from the real class (rows) is shown in each cell. High values along the diagonal represent correct classifications, with particularly strong performance on classes like "Normal" (8923), "Ransomware" (6456), and "Injection" (6444). Minimal off-diagonal values suggest low misclassification rates, demonstrating the excellent precision and efficacy of the model in differentiating between various assault types and typical behavior.

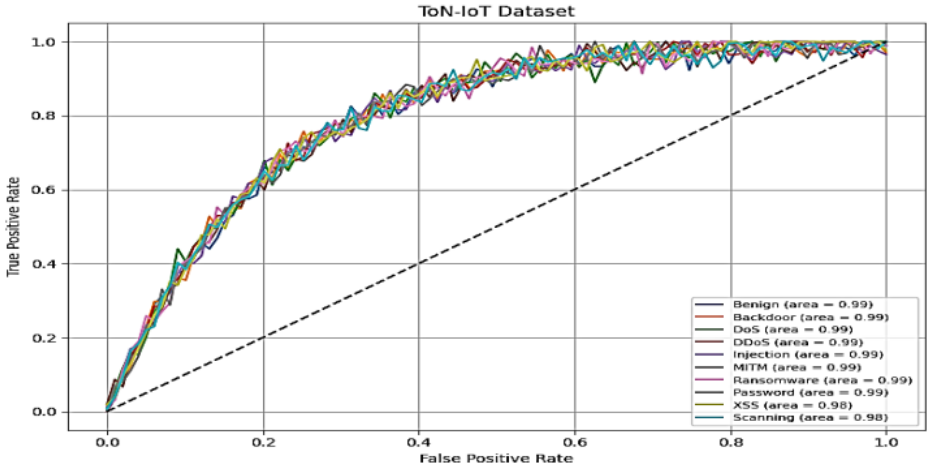

Fig 7: Roc Curve for LSTM

The ROC curves for an assessed multi-class classification model are shown in Figure 7 on the ToN-IoT dataset, covering various attack types and benign traffic. Each colored line represents a different class, with A comparison between the TP Rate and the FP Rate. The ROC curves show substantial discriminating power across all classes since they are located considerably above the diagonal baseline. The AUC values are impressively high, mostly around 0.99, with the lowest being 0.98 for XSS and Scanning, highlighting the model's excellent overall performance and robustness in detecting both normal and malicious activities.

Table 2: Comparison Analysis between base and proposed Model performance for intrusion detection system.

Matrix	LSTM	DBN[20]
Accuracy	99.41	80.58
Precision	99.35	88.10
Recall	99.32	80.58
F1-score	99.33	84.08

A comparison of the baseline DBN model and the suggested LSTM model in Table III shows a notable increase in performance across all assessment measures. The LSTM achieved a notably higher accuracy of 99.41%, compared to 80.58% for DBN, indicating superior overall classification performance. Precision improved from 88.10% with DBN to 99.35% with LSTM, suggesting that LSTM produces fewer false positives. The LSTM model showed improved recall performance because it advanced from 80.58% to 99.32% in identifying pertinent instances. The F1-score which reconciles accuracy and recall values showed significant growth from 84.08% to 99.33% confirming the strong reliability of LSTM model. These results clearly establish LSTM as a more reliable and accurate model compared to the DBN baseline.

The suggested LSTM model searches for and detects long-term temporal relationships, it has essential features for efficient data preservation appropriate for sequential pattern recognition applications. F1-score measurement findings, precision, accuracy, and recall were the foundation of the model's strength. While the basic DBN is unable to comprehend temporal dynamics, the LSTM retains crucial contextual information over time, resulting in worse performance results. As a result, there are fewer false positives and negatives, more accurate and consistent forecasts, and a more dependable model for practical applications.

5. Conclusion And Future Scope

According to research findings, the creation of intelligent automated business systems from conventional industrial settings is made possible by the combination of Industrial IoT with cloud computing and sophisticated analytics. The research contributed an innovative solution to enhance IoT security through the implementation of LSTM as a part of Deep Learning-based anomaly detection methods. The proposed LSTM-based model achieved remarkable performance on ToN-IoT test data by demonstrating 99.41% accuracy while maintaining 99.35% precision and 99.32% recall and 99.33% F1-score in IoT threat identification. According to research findings, LSTM models, which have outstanding scalability and robustness characteristics, can detect IoT network activities by differentiating between safe and dangerous operations. The ability of updated LSTM models to identify longer network traffic behavior patterns allowed researchers to outperform DBN models in attack detection. Advanced pre-processing methods must be implemented to solve class imbalance problems. The ToN-IoT dataset's unbalanced distribution of classes could result in incorrect identification of scarce attack types. Large networks face scalability challenges due to computational complexity of the model. The model's performance efficiency needs improvement according to future research findings. Total strategies must be implemented for tackling class imbalance problems because they pose a fundamental requirement. Testing in real-time IoT environments would further validate its robustness.

References

[1] J. King and A. I. Awad, “A distributed security mechanism for Resource-Constrained IoT Devices,” *Inform.*, 2016.

[2] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, “Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches,” *Internet of Things (Netherlands)*, 2019, doi: 10.1016/j.iot.2019.100059.

[3] E. Bertino, K. K. R. Choo, D. Georgakopolous, and S. Nepal, “Internet of things (IoT): Smart and secure service delivery,” *ACM Trans. Internet Technol.*, 2016, doi: 10.1145/3013520.

[4] G. Thamilarasu and S. Chawla, “Towards deep-learning-driven intrusion detection for the internet of things,” *Sensors (Switzerland)*, 2019, doi: 10.3390/s19091977.

[5] S. T. Bakhsh, S. Alghamdi, R. A. Alsemmeari, and S. R. Hassan, “An adaptive intrusion detection and prevention system for Internet of Things,” *Int. J. Distrib. Sens. Networks*, 2019, doi: 10.1177/1550147719888109.

[6] A. Ghosh, D. Chakraborty, and A. Law, “Artificial intelligence in Internet of things,” *CAAI Trans. Intell. Technol.*, vol. 3, no. 4, pp. 208–218, Dec. 2018, doi: 10.1049/trit.2018.1008.

[7] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, “Intrusion detection systems for IoT-based smart environments: a survey,” *Journal of Cloud Computing*. 2018. doi: 10.1186/s13677-018-0123-6.

[8] A. Alshammari, M. A. Zohdy, D. Debnath, and G. Corser, “Classification Approach for Intrusion Detection in Vehicle Systems,” *Wirel. Eng. Technol.*, 2018, doi: 10.4236/wet.2018.94007.

[9] J. hua Li, “Cyber security meets artificial intelligence: a survey,” *Frontiers of Information Technology and Electronic Engineering*. 2018. doi: 10.1631/FITEE.1800573.

[10] V. Kolluri, “A Comprehensive Analysis on Explainable and Ethical Machine: Demystifying Advances in Artificial Intelligence,” *TIJER - Int. Res. Journals*, vol. 2, no. 7, pp. 2349–9249, 2015.

[11] [11] J. Ordóñez, P. Ameigeiras, D. Lopez, J. Ramos, J. Lorca, and J. Folgueira, “Network Slicing for 5G with SDN/NFV: Concepts, Architectures and Challenges,” *IEEE Commun. Mag.*, vol. 55, 2017, doi: 10.1109/MCOM.2017.1600935.

[12] D. Li, L. Deng, M. Lee, and H. Wang, “IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning,” *Int. J. Inf. Manage.*, vol. 49, no. October 2018, pp. 533–545, 2019, doi: 10.1016/j.ijinfomgt.2019.04.006.

[13] V. Kolluri, "A Pioneering Approach To Forensic Insights: Utilization AI for Cybersecurity Incident Investigations," *Int. J. Res. Anal. Rev.*, vol. 3, no. 3, 2016.
[14] P. Van Huong, L. D. Thuan, L. T. Hong Van, and D. V. Hung, "Intrusion detection in IoT systems based on deep learning using convolutional neural network," in *Proceedings - 2019 6th NAFOSTED Conference on Information and Computer Science, NICS 2019*, 2019. doi: 10.1109/NICS48868.2019.9023871.
[15] M. Roopak, G. Y. Tian, and J. Chambers, "Deep Learning Models for Cyber Security in IoT Networks," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, Jan. 2019, pp. 0452–0457. doi: 10.1109/CCWC.2019.8666588.
[16] I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy, and H. Ming, "AD-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC 2019*, 2019. doi: 10.1109/CCWC.2019.8666450.
[17] B. Roy and H. Cheung, "A Deep Learning Approach for Intrusion Detection in Internet of Things using Bi-Directional Long Short-Term Memory Recurrent Neural Network," in *2018 28th International Telecommunication Networks and Applications Conference, ITNAC 2018*, 2018. doi: 10.1109/ATNAC.2018.8615294.
[18] F. Ertam, I. F. Kilinçer, and O. Yaman, "Intrusion detection in computer networks via machine learning algorithms," in *IDAP 2017 - International Artificial Intelligence and Data Processing Symposium*, 2017. doi: 10.1109/IDAP.2017.8090165.
[19] E. Hodo *et al.*, "Threat analysis of IoT networks using artificial neural network intrusion detection system," in *2016 International Symposium on Networks, Computers and Communications, ISNCC 2016*, 2016. doi: 10.1109/ISNCC.2016.7746067.
[20] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," *IEEE Trans. Emerg. Top. Comput. Intell.*, vol. 2, no. 1, pp. 41–50, 2018, doi: 10.1109/TETCI.2017.2772792.
[21] Kalla, D., & Samiuddin, V. (2020). Chatbot for medical treatment using NLTK Lib. *IOSR J. Comput. Eng*, *22*, 12.
[22] Kuraku, S., & Kalla, D. (2020). Emotet malware a banking credentials stealer. *Iosr J. Comput. Eng*, *22*, 31-41.