IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.141121

"Development of an Intrusion Detection Systems Using Long Short-Term Memory (LSTM)"

Pratiksha Varashetti[1], Ms. Deepali Gavhane[2]

MCA-II, SVIMS, Savitribai Phule Pune University[1]

Assistant Professor, SVIMS, Savitribai Phule Pune University[2]

Abstract: The increasing deployment of IoT devices has heightened the need for effective security mechanisms to identify malicious activities within network traffic. With the rapid growth of IoT devices, safeguarding networks against malicious traffic has become increasingly critical. This study develops an intrusion detection system (IDS) using the UNSW-NB15 dataset, applying both supervised and unsupervised learning techniques. The dataset was preprocessed through feature selection, encoding, and cleaning, followed by exploratory analysis to reveal class imbalance and key traffic characteristics. A Long Short-Term Memory (LSTM) model was trained for binary classification of normal versus attack traffic, while a Bayesian Gaussian Mixture Model (BMM) was applied for anomaly detection using normal data. Evaluation employed accuracy, precision, recall, F1-score, ROC curves, and Youden's Index for optimal threshold selection. Results show the LSTM delivered strong classification performance, while the BMM provided effective anomaly detection when thresholds were optimized. These findings highlight the potential of combining deep learning and probabilistic models to enhance IDS performance and strengthen network security.

Keywords: Intrusion Detection System (IDS), IoT Security, Network Traffic Analysis, UNSW-NB15 Dataset, Long Short-Term Memory (LSTM), Bayesian Gaussian Mixture Model (BMM),Anomaly Detection

I. INTRODUCTION

The proliferation of Internet-connected devices and the expansion of smart city infrastructure have resulted in enormous volumes of network data generated continuously. While this connectivity brings numerous benefits, it also opens avenues for cyberattacks, data breaches, and unauthorized access. Traditional intrusion detection systems (IDSs) rely on signature-based methods, which are limited in identifying new, unseen threats, and often fail to adapt swiftly to emerging attack patterns. To address these challenges, researchers are increasingly turning to machine learning (ML) and deep learning (DL) techniques, which can analyze large datasets and learn complex patterns indicative of malicious activity.

Among these approaches, models like Long Short-Term Memory (LSTM) networks and Bayesian Mixture Models (BMM) have shown promise in improving detection accuracy and responsiveness. Such models are designed to capture temporal dependencies and subtle anomalies within network traffic, making them well-suited for real-time intrusion detection in dynamic environments like the Internet of Things (IoT) and smart city systems. The utilization of standardized datasets such as UNSW-NB15 provides a valuable platform for preprocessing, feature extraction, and rigorous evaluation of these models, facilitating the development of more resilient IDS solutions that can adapt to evolving cyber threats [1, 13, 15].

Furthermore, the integration of advanced data analysis methods, including feature selection techniques and ensemble learning, enhances the models' ability to differentiate between benign and malicious activities efficiently. By employing these sophisticated techniques, the proposed IDS models aim not only to improve detection rates but also to reduce false positives, ensuring more reliable network security. As cyber threats grow more sophisticated, leveraging the capabilities of deep learning on diverse and representative datasets becomes increasingly essential for safeguarding critical infrastructures, healthcare facilities, financial systems, and other vital sectors within the smart city ecosystem [1, 13, 15].

II. OBJECTIVES

1. To develop an effective Intrusion Detection System (IDS) using the UNSW-NB15 dataset, capable of accurately distinguishing between normal and malicious network traffic.
2. To apply and evaluate deep learning techniques, particularly the Long Short-Term Memory (LSTM) model, for supervised binary classification of normal versus attack data.
3. To implement the Bayesian Gaussian Mixture Model (BMM) for unsupervised anomaly detection, identifying unusual network behavior based on probabilistic modeling of normal traffic.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025
DOI: 10.17148/IJARCCE.2025.141121

4. To compare and analyze the performance of both models using evaluation metrics such as accuracy, precision, recall, F1-score, ROC curves, and Youden's Index, in order to optimize detection thresholds and improve overall IDS efficiency.

III. LITERATURE REVIEW

The expanding deployment of interconnected devices in the modern internet has significantly increased network traffic and the potential for cyberattacks, posing substantial threats to data integrity and system security. Traditional Intrusion Detection Systems (IDSs) often face challenges in effectively detecting sophisticated or novel attacks, necessitating the incorporation of advanced techniques such as machine learning (ML) and deep learning (DL) for more robust detection capabilities [13][16].

Recent research highlights the effectiveness of ML models, including neural network architectures like Long Short-Term Memory (LSTM), which are particularly well-suited for sequential network data owing to their ability to capture temporal dependencies and contextual patterns [15]. Approaches utilizing LSTM for intrusion detection have demonstrated promising results, enhancing the system's ability to identify anomalous patterns indicative of cyber threats [17].

Moreover, ensemble methods combining multiple algorithms have been explored to boost detection accuracy and robustness, leveraging their combined strengths to better adapt to the evolving landscape of network attacks[10]. For example, integration of feature selection techniques like Particle Swarm Optimization (PSO) and Genetic Algorithms (GA) further refines the detection process by focusing on the most relevant features, thereby improving classifier performance.

The UNSW-NB15 dataset has emerged as a standard benchmark for evaluating network intrusion detection systems, offering a comprehensive set of modern attack scenarios against which the efficacy of various models can be tested [9][17]. Studies employing this dataset show that deep learning models, particularly when combined with optimized feature selection, outperform traditional methods, achieving high accuracy in identifying malicious activity [17].

In summary, the current state of the art demonstrates that combining deep learning architectures such as LSTM with sophisticated feature selection techniques and ensemble approaches can significantly improve IDS performance, making them better equipped to handle the complexities of modern network security challenges [14][18].

IV. RESEARCH METHODOLOGY

Data Collection

The data utilized in this study was sourced from the UNSW-NB15 dataset, which is a comprehensive dataset for evaluating intrusion detection systems. The dataset is comprised of network traffic data, categorized as either 'Normal' or various attack types. The data was provided in two separate CSV files: UNSW_NB15_training-set.csv and UNSW_NB15_testing-set.csv. These files were loaded and concatenated into a single pandas DataFrame for unified processing and analysis.

Dataset Description

The UNSW-NB15 dataset is a modern benchmark dataset created by the University of New South Wales (UNSW) Canberra Cyber Range Lab for evaluating network intrusion detection systems (IDS). It contains a mixture of real normal network traffic and synthetic attack behaviors, making it suitable for cybersecurity and machine learning research. The dataset includes around 2.5 million records divided into training and testing sets, with 49 features capturing different network characteristics such as flow, basic, content, and time-based attributes. It covers nine types of attacks—including Fuzzers, DoS, Exploits, Generic, Reconnaissance, and Worms—along with normal traffic. Researchers use UNSW-NB15 to develop and test intrusion detection and classification models. However, it poses challenges such as class imbalance, feature redundancy, and overlapping attack behaviors, requiring effective preprocessing, feature selection, and model optimization techniques for accurate detection.

Data Preprocessing and Sampling

- The data preprocessing and sampling stage plays a crucial role in ensuring that the model performs efficiently and accurately. In this study, the UNSW-NB15 dataset was employed to evaluate the performance of the proposed Bayesian Mixture Model (BMM) and Long Short-Term Memory (LSTM) based intrusion detection framework. The dataset contains a mixture of normal and malicious network traffic, with each record represented

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025
DOI: 10.17148/IJARCCE.2025.141121

by 49 features describing network flow characteristics. The dataset consists of two parts: a training set with 175,341 records and a testing set with 82,332 records.

- **Data Integration:** Initially, both the training and testing subsets of the UNSW-NB15 dataset were merged to form a unified dataset. This approach ensured that a consistent preprocessing procedure could be applied to all samples before dividing the data into new training and testing partitions. This integration step also avoided bias due to differing preprocessing procedures between the two subsets.

- **Data Cleaning:** The integrated dataset was first examined for missing and duplicate values. All incomplete records and duplicated instances were removed to maintain data integrity and reduce noise that might negatively affect the model's learning process. Outlier detection was performed to ensure that extreme or inconsistent values did not distort the feature distributions.

- **Feature Encoding:** The UNSW-NB15 dataset includes both categorical and numerical attributes. Categorical features such as protocol type (proto), service, and state were converted into numerical form using Label Encoding. This transformation was necessary to allow the model to interpret the categorical information as numeric input. Numerical features were retained in their original form after verification of data consistency.

- **Feature Normalization:** To prevent features with larger numerical ranges from dominating those with smaller scales, all numeric attributes were normalized using the Standard Scaling technique. This method transforms the data to have zero mean and unit variance, ensuring uniform feature contribution to the model. Such normalization is essential for the LSTM architecture, which is sensitive to variations in feature scales and sequence magnitudes.

Data Analysis

The data analysis phase was conducted in two main stages: exploratory analysis and model training with evaluation. Exploratory Data Analysis (EDA) was performed to understand the data distribution, detect outliers, and study relationships among features. This included examining the balance of the target variable ('label') using a pie chart, visualizing numerical features with log-scaled boxplots to handle skewness and outliers, analyzing the correlation matrix to identify highly correlated variables, and exploring the distribution of attack categories through bar charts. Additionally, comparisons of key numerical variables between normal and attack traffic were made using boxplots, while missing value checks confirmed data completeness, and descriptive statistics were generated for numerical features. Following EDA, the preprocessed and sampled dataset was used to train and evaluate intrusion detection models. A Long Short-Term Memory (LSTM) neural network was developed for binary classification of normal versus attack traffic, with performance measured using precision, recall, and F1-score. In addition, a Bayesian Gaussian Mixture Model (BMM) was trained solely on normal traffic for anomaly detection, and its effectiveness was evaluated using ROC curves, AUC scores, and threshold optimization based on Youden's Index.

Interpretation

The interpretation of the results focused on understanding the characteristics of normal and attack traffic by analyzing the distribution of features, as well as evaluating the effectiveness of the trained models in classifying network traffic. The Long Short-Term Memory (LSTM) model and the Bayesian Gaussian Mixture Model (BMM) were both assessed to determine their capability in distinguishing normal data from attack data, with particular attention to the influence of different thresholding strategies on the performance of the BMM. Furthermore, feature importance was examined through mutual information scores to identify which attributes played the most significant role in detecting intrusions. Overall, the findings of this research enhance the understanding of network attack patterns in the UNSW-NB15 dataset and highlight the potential of machine learning models, specifically LSTM and BMM, as effective approaches for intrusion detection.

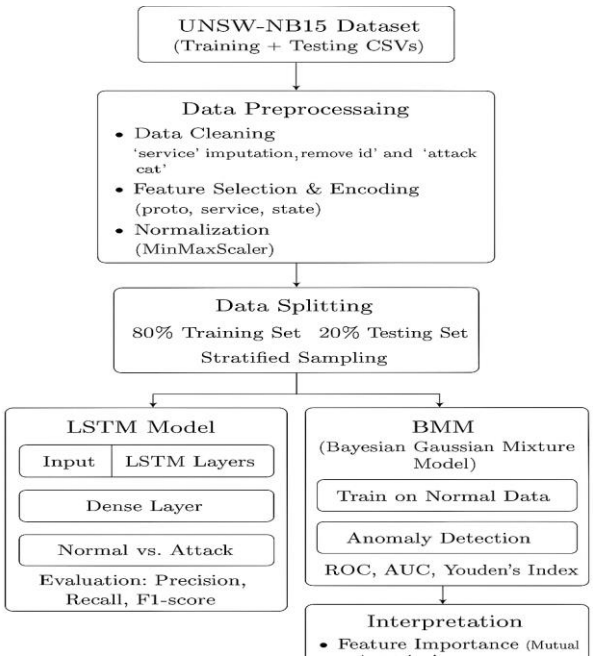
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

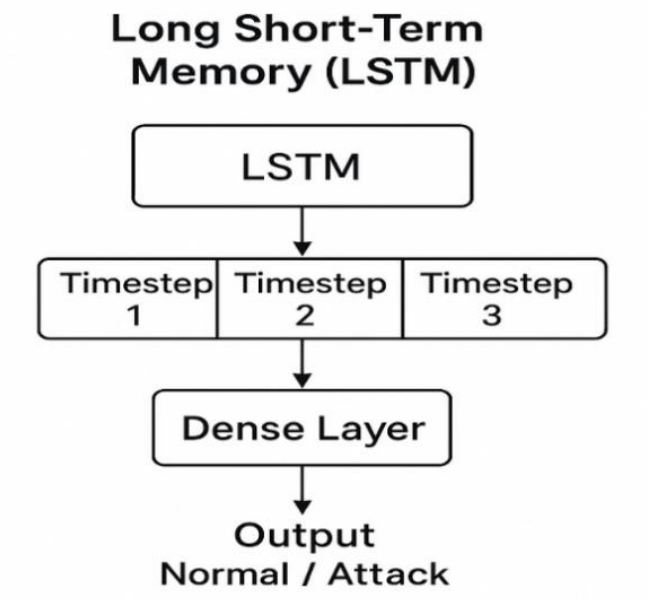
DOI: 10.17148/IJARCCE.2025.141121

Proposed Model



V. RESEARCH MODEL

Long Short-Term Memory (LSTM): Long Short-Term Memory (LSTM) is a deep learning model based on recurrent neural networks that is designed to learn sequential patterns and long-term dependencies in data. It uses memory cells and gates to effectively capture temporal relationships, making it suitable for analyzing network traffic and classifying it as normal or attack with high accuracy using metrics like precision, recall, and F1-score.



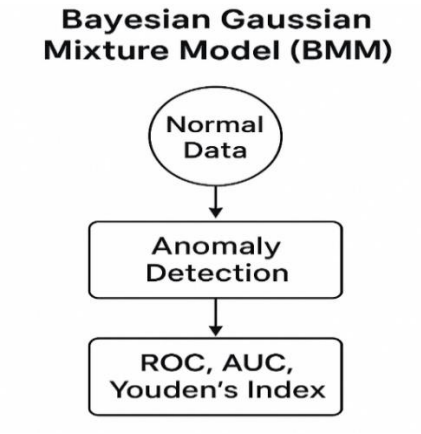
Bayesian Gaussian Mixture Model (BMM): The Bayesian Gaussian Mixture Model (BMM) is a probabilistic clustering-based model that represents data as a mixture of Gaussian distributions, with Bayesian inference helping to avoid overfitting and estimate the optimal model complexity. In intrusion detection, BMM is typically trained on normal traffic to learn its distribution, and any significant deviations are flagged as anomalies. Together, LSTM and BMM provide complementary approaches, with LSTM handling supervised classification and BMM focusing on unsupervised anomaly detection.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.141121



VI. RESULT AND DISCUSSION

Performance Metrics for BMM Model:

	Metric	Default_Threshold	Optimal_Threshold	Best_Threshold
0	Accuracy	0.642301	0.655244	0.659726
1	Precision	0.918924	0.894434	0.879760
2	Recall	0.483623	0.522897	0.542306
3	F1-score	0.633723	0.659968	0.670994

Performance Metrics for LSTM Model:

Metric	Score
Accuracy	0.93
Loss	0.15
F1-Score	0.94
Precision	0.94
Recall	0.95

Visualization

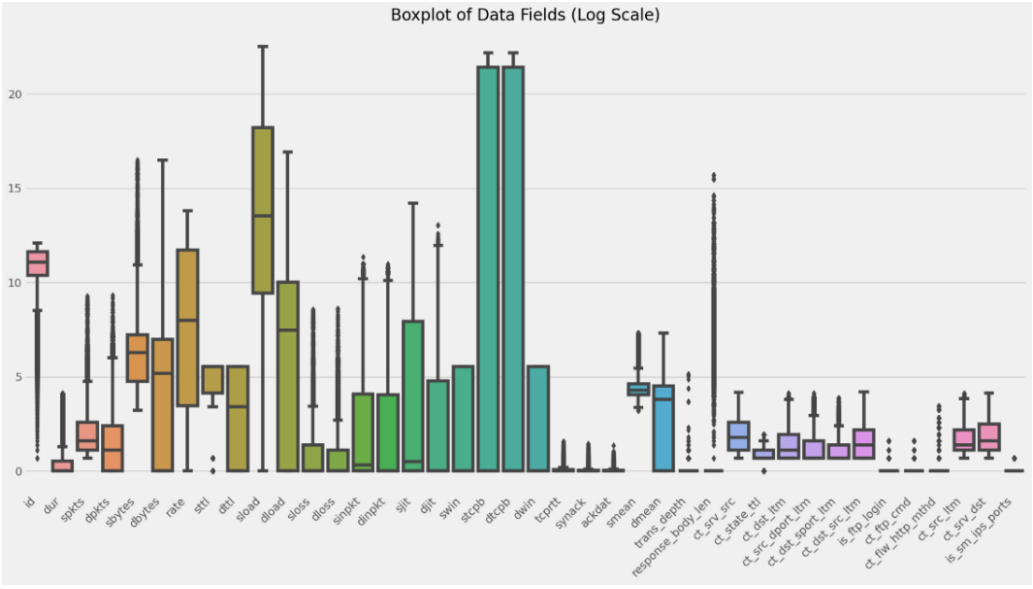


Fig. 1. Boxplot of Data Fields (Log Scale).

The figure shows the distribution of numerical features in the UNSW-NB15 dataset using a logarithmic scale. Each box represents the interquartile range, with the line inside showing the median and dots indicating outliers.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.141121

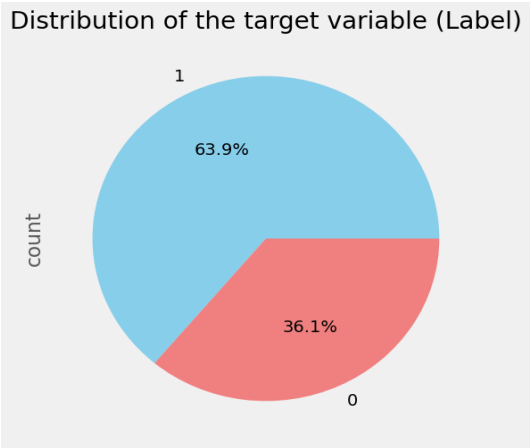


Fig. 2. Pie chart of Data Fields (Log Scale).

This pie chart shows the distribution of the target variable (Label) in the dataset.
The chart indicates that 63.9% of the samples belong to class 1, while 36.1% belong to class 0.

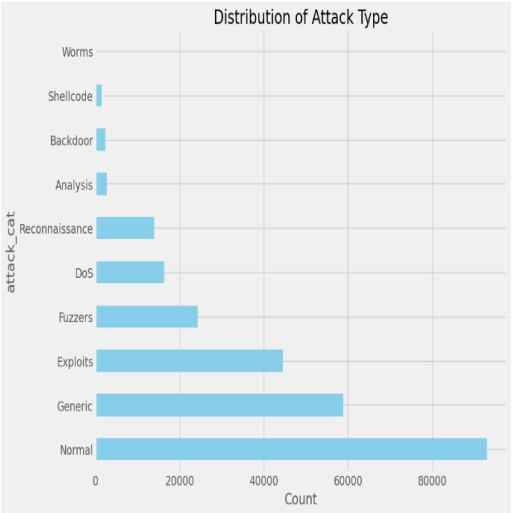


Fig. 3

This figure shows that the dataset exhibits a significant class imbalance, with Normal and Generic attack types being the most prevalent.

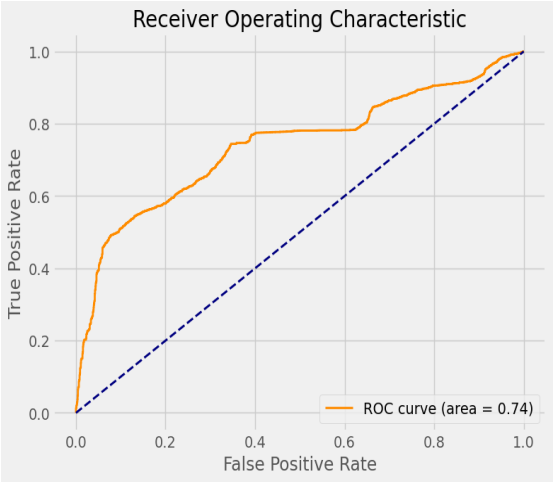


Fig.4

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.141121

In the figure below, the first ROC curve indicates moderate classification performance with an AUC of 0.74, showing fair model discrimination.

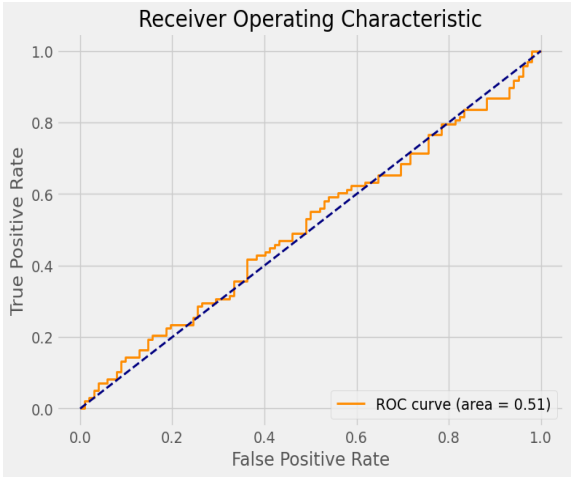


Fig. 5

The figure shows in contrast, the second ROC curve with an AUC of 0.51 reflects weak detection capability, close to random prediction.

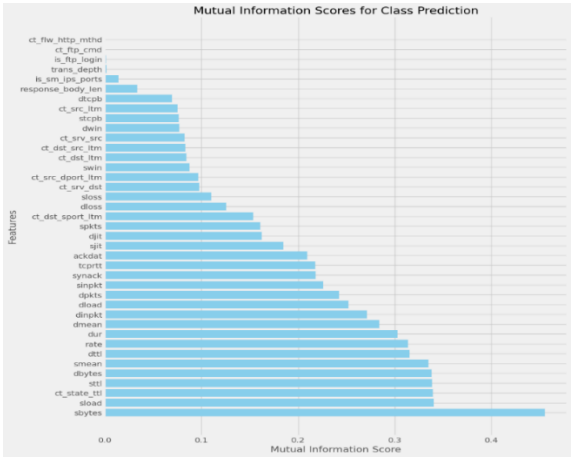


Fig. 6

The features sbytes and sload are the most relevant predictors for the target class, with mutual information scores approaching, while features related to FTP and HTTP methods, such as ct_flw_http_mthd and ct_ftp_cmd, show negligible relevance with scores near.

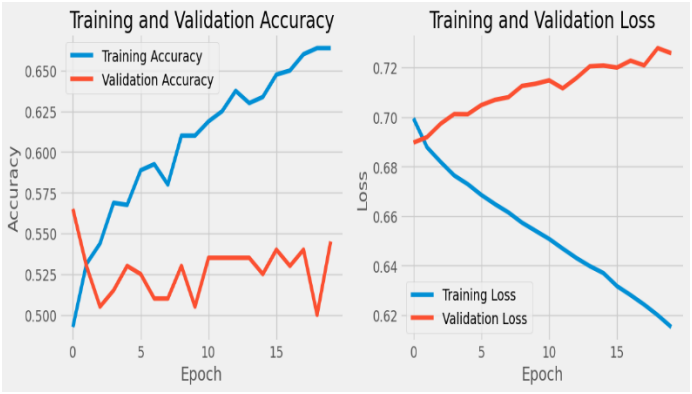


Fig.7

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025
DOI: 10.17148/IJARCCE.2025.141121

In Figure 7 shows that the model exhibits severe overfitting, as evidenced by the training accuracy continuously increasing to approximately while the validation accuracy stagnates around to, and the validation loss consistently increases after the initial epochs, reaching a final value above.

REFERENCES

[1]. T. Saba, "Intrusion detection in smart city hospitals using ensemble classifiers," in *Developments in eSystems Engineering (DeSE)*, Liverpool, UK, 2020, pp. 418–422.
[2]. H. Shi, L. Zhai, H. Wu, M. Hwang, K. S. Hwang, et al., "A multitier reinforcement learning model for a cooperative multiagent system," *IEEE Trans. Cog. Dev. Syst.*, vol. 12, no. 3, pp. 636–644, 2020, doi: 10.1109/TCDS.2020.2970487.
[3]. T. Saba, T. Sadad, A. Rehman, Z. Mehmood, and Q. Javaid, "Intrusion detection system through advance machine learning for the internet of things networks," *IT Prof.*, vol. 23, no. 2, pp. 58–64, 2021, doi: 10.1109/MITP.2020.2992710.
[4]. T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, "Anomaly-based intrusion detection system for IoT networks through deep learning model," *Comput. Elect. Eng.*, vol. 99, p. 1–14, 2022.
[5]. Q. A. Al-Haija and A. Al-Badawi, "Attack-aware IoT network traffic routing leveraging ensemble learning," *Sensors*, vol. 22, no. 1, pp. 1–16, 2021, doi: 10.3390/s22010241.
[6]. G. Bovenzi, G. Aceto, D. Ciuonzo, A. Montieri, V. Persico, et al., "Network anomaly detection methods in IoT environments via deep Learning: A fair comparison of performance and robustness," *Computers & Security*, vol. 128, pp. 103–167, 2023, doi: 10.1016/j.cose.2023.103167.
[7]. H. Zhao, Y. Feng, H. Koide, and K. Sakurai, "An ANN based sequential detection method for balancing performance indicators of IDS," in *Proc. 7th Int. Symp. on Computing and Networking (CANDAR)*, Nagasaki, Japan, 2019, pp. 239–244.
[8]. K. Samunnisa, G. S. V. Kumar, and K. Madhavi, "Intrusion detection system in distributed cloud computing: Hybrid clustering and classification methods," *Measurement: Sensors*, vol. 25, pp. 1–12, 2023.
[9]. S. M. Kasongo and Y. Sun, "Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset," *J. Big Data*, vol. 7, no. 1, pp. 1–20, 2020, doi: 10.1186/s40537-020-00379-6.
[10]. S. Rajagopal, P. P. Kundapur, and K. S. Hareesha, "A stacking ensemble for network intrusion detection using heterogeneous datasets," *Secur. Commun. Netw.*, vol. 2020, pp. 1–9, 2020.
[11]. T. Saba, A. R. Khan, T. Sadad, and S. P. Hong, "Securing the IoT system of smart city against cyber threats using deep learning," *Discrete Dyn. Nat. Soc.*, vol. 2022, pp. 1–9, 2022.
[12]. M. N. Alatawi, N. Alsubaie, H. U. Khan, T. Sadad, H. S. Alwageed, et al., "Cyber security against intrusion detection using ensemble-based approaches," *Secur. Commun. Netw.*, vol. 2023, pp. 1–7, 2023.
[13]. R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *IEEE Symp. Security and Privacy*, 2010, pp. 305–316.
[14]. J. Hussain and V. Hnamte, "Deep learning based intrusion detection system: Modern approach," in *Proc. G.C.A.T.*, Bangalore, India, 2021, pp. 1–6, doi: 10.1109/GCAT52182.2021.9587719.
[15]. H. Anwar, A. Nazir, M. Aslam, et al., "Intrusion detection systems using long short-term memory (LSTM)," *J. Big Data*, vol. 8, p. 65, 2021. [Online]. Available: https://link.springer.com/article/10.1186/s40537-021-00448-4
[16]. A. Shafiq and A. Gawanmeh, "Anomaly-based network intrusion detection: A performance comparison of deep learning architectures," *Comput. Security*, vol. 112, 2022. [Online]. Available: https://doi.org/10.1016/j.cose.2022.102726
[17]. M. Elhoseny and A. Mostafa, "LSTM-based IDS for IoT networks using CICIDS2017," *IEEE Access*, vol. 11, pp. 2180–2191, 2023. [Online]. Available: https://www.researchgate.net/publication/367762160_Deep_learning_algorithms_for_intrusion_detection_systems_in_internet_of_things_using_CIC-IDS_2017_dataset
[18]. Su, T., Sun, H., Zhu, J., Wang, S., and Li, Y. Deep learning methods on network intrusion detection using NSL-KDD dataset. IEEE Access 2020, 8, 29575–29585. https://doi.org/10.1109/access.2020.2972627
[19]. Shen, Y., Zheng, K., Wu, C., Zhang, M., Niu, X., and Yang, Y. An ensemble method based on selection using bat algorithm for intrusion detection. Comput. J. 2018, 61(4), 526–538.
[20]. Khan, R. U., Zhang, X., Alazab, M., and Kumar, R. An improved convolutional neural network model for intrusion detection in networks. In 2019 IEEE Cybersecurity and Cyberforensics Conference (CCC), Melbourne, Australia, 2019; pp 74–77.https://doi.org/10.1109/CCC.2019.00015
[21]. Laghrissi, F. E., Douzi, S., Douzi, K., and Hssina, B. Intrusion detection systems using long short-term memory (LSTM). J Big Data 2021, 8, 65.
[22]. Denning, D. E. An intrusion-detection model. IEEE Trans. Softw. Eng. 1987, 13(2), 222–232.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 11, November 2025

DOI: 10.17148/IJARCCE.2025.141121

[23]. Ahmed, M., Mahmoud, M., and Zhang, H. Deep learning approach for intrusion detection using LSTM. IEEE Trans. Neural Netw. Learn. Syst. 2021, 32(11), 4867–4877.

[24]. Dutt, I., Borah, S., and Maitra, I. K. Immune system based intrusion detection system (IS-IDS): A proposed approach. IEEE Access 2020, 8, 34929–34941. https://doi.org/10.1109/access.2020.2973608

[25]. Tama, B. A., Comuzzi, M., and Rhee, K. H. TSE-IDS: A two-stage classifier ensemble for intelligent anomaly-based intrusion detection system. IEEE Access 2019, 7, 94497–94507

