Enhancing Cloud Data Center Security through Deep Learning: A Comparative Analysis of RNN, CNN, and LSTM Models for Anomaly and Intrusion Detection

Shimaa A. Ahmed
Department of Electrical Engineering, College of Engineering, Northern Border University, Arar, Saudi Arabia
shaima.ahmad@nbu.edu (corresponding author)

Entisar H. Khalifa
Department of Computer Science, College of Science, Northern Border University, Arar, Saudi Arabia
entisar.osman@nbu.edu.sa

Majid Nawaz
Department of Computer Science, College of Science, Northern Border University, Arar, Saudi Arabia
majed.nawaz@nbu.edu.sa

Faroug A. Abdalla
Department of Computer Science, College of Science, Northern Border University, Arar, Saudi Arabia
faroug.abdalla@nbu.edu.sa

Ashraf F. A. Mahmoud
Department of Computer Science, College of Science, Northern Border University, Arar, Saudi Arabia
ashraf.abubaker@nbu.edu.sa

Received: 30 October 2024 | Revised: 24 November 2024, 28 November 2024, and 3 December 2024 | Accepted: 22 December 2024

ABSTRACT

Cloud data centers form the backbone of modern digital ecosystems, enabling critical operations for businesses, governments, and individuals around the world. However, their high connectivity and complexity make them prime targets for cyberattacks, leading to service disruptions and data breaches. This paper investigates the use of deep learning techniques, namely Recurrent Neural Networks (RNNs), Convolutional Neural Networks (CNNs), and Long Short-Term Memory (LSTM) networks, to enhance cloud data center security. By employing these models for anomaly detection and intrusion prevention, the study performs a comparative analysis. The results indicate that the LSTMs achieved the highest ROC AUC score (0.90), demonstrating better detection of persistent threats. These findings highlight the potential of deep learning to revolutionize cloud security by providing scalable, accurate, and proactive measures against evolving cyber threats.

Keywords-cloud data centers; deep learning; downtime; cyberattacks; predictive analytics; anomaly detection; intrusion prevention

I. INTRODUCTION

Cloud data centers are essential for providing scalable, reliable, and on-demand computing resources to various industries, including healthcare, finance, and education. However, their complexity and widespread use make them attractive targets for cyberattacks, with incidents such as ransomware and Distributed Denial-of-Service (DDoS) attacks becoming more frequent and sophisticated. A 2023 IBM report revealed that the average cost of data breaches in cloud environments exceeded $4.45 million [1], highlighting the urgent need for advanced cybersecurity measures and emphasizing the importance of Intrusion Detection Systems (IDS), which leverage diverse technologies, data sources, and detection times [2]. High-profile security breaches further underscore the vulnerabilities inherent in cloud systems. For example, the 2020 Zoom breach, which exposed more than 500,000 user accounts, demonstrated the devastating impact of compromised cloud security on user trust and operational continuity [3]. Similarly, large-scale DDoS attacks on cloud platforms have caused prolonged outages, resulting in significant financial and reputational damage for affected organizations. The dynamic and evolving nature of these threats calls for adaptive and intelligent cybersecurity frameworks to address the unique challenges faced by cloud environments. Conventional security methods, such as signature-based IDS and rule-based firewalls, have traditionally served as the first line of defense against cyber threats. These methods rely on predefined patterns or rules to detect malicious activities. While effective against known threats, they falter when faced with zero-day vulnerabilities, polymorphic malware, and insider attacks [4]. For instance, signature-based IDS cannot detect novel attack signatures, leaving systems vulnerable to emerging threats. Additionally, these systems often suffer from high false-positive rates, leading to alert fatigue and undermining the confidence of security teams in their effectiveness.

Traditional machine-learning techniques, such as SVMs, Random Forests (RF), and Decision Trees (DT), are commonly used for anomaly detection. However, they struggle with the vast and varied data in modern cloud and IoT environments. These techniques also require intensive feature engineering and cannot handle sequential or high-dimensional data effectively, limiting their ability to detect complex attacks [5]. Recent research has highlighted the need for real-time anomaly detection and class imbalance handling. In [6], a weighted class classification scheme was used, combining a supervised algorithm with historical network data and an iterative approach to boost detection accuracy, particularly for rare attacks. The use of a weight optimization algorithm enhances overall performance, with testing on the UNSW dataset showing superior results compared to existing methods. Generative Adversarial Networks (GANs) have proven effective in generating synthetic data, addressing data imbalance and clustering challenges in training machine learning models for Network IDSs (NIDSs). High performance has been achieved using GANs across datasets such as UNSW-NB15, NSL-KDD, and BoT-IoT, with results matching or exceeding those of traditional methods. This approach reduces the reliance on real-world data and offers a flexible and scalable solution. These findings contribute to enhancing anomaly and intrusion detection in cloud environments by integrating generative data techniques [7].

In [7], a novel architecture was proposed that integrated cloud computing with advanced machine learning techniques to address these challenges. This approach introduced a Polynomial Radial Basis Function (PRBF) kernel to improve the classification accuracy of SVMs over traditional kernels. The proposed PRBF-SVM model was benchmarked against Logistic Regression (LR), standard SVMs, and XGBoost, demonstrating enhanced detection performance through optimized hyperparameter tuning. Furthermore, the integration of cloud services facilitates the efficient offloading of computationally intensive tasks, ensuring scalability and real-time threat detection. This combined framework provides a robust and scalable solution for securing IoT and cloud environments against evolving cyber threats [8]. Several machine learning algorithms, including LR, DT, Naive Bayes (NB), RF, AdaBoost, and XGBoost, have been employed for ransomware detection, focusing on metrics such as accuracy, precision, recall, F1-score, and computational performance. These approaches highlight the critical need for efficient and accurate detection models capable of working effectively in real-time scenarios [9]. In [10], a real-time anomaly detection algorithm using Hierarchical cache (HTM) was employed to address challenges such as concept drift and automation in data flow. This approach was evaluated on the Numenta Anomaly Benchmark (NAB) using real-world labeled data, demonstrating its effectiveness and underscoring the need for continuous learning models in line with research in deep learning for anomaly detection in cloud environments.

Deep learning has revolutionized the field of cybersecurity by introducing models that can automatically learn and adapt to complex patterns in data. Unlike traditional machine learning approaches, deep learning models can process unstructured and sequential data, making them well-suited for modern cybersecurity applications [11, 12]. Recurrent Neural Networks (RNNs) are particularly adept at analyzing temporal data, such as activity logs, to detect behavioral anomalies [13]. Long Short-Term Memory (LSTM) networks, a specialized form of RNNs, excel at capturing long-term dependencies, allowing the detection of persistent threats such as insider misuse and gradual anomalies [14]. Similarly, Convolutional Neural Networks (CNNs) have demonstrated remarkable effectiveness in analyzing high-dimensional data, such as network traffic, for real-time anomaly detection [15].

Despite these advances, existing research often focuses on isolated aspects of cloud security, such as anomaly detection or intrusion detection, without addressing the full spectrum of threats encountered in real-world cloud environments. Furthermore, many studies fail to provide a comparative analysis of deep learning models across multiple evaluation metrics, limiting their applicability in diverse scenarios. This study addresses these gaps by proposing a unified framework that combines anomaly and intrusion detection techniques utilizing state-of-the-art datasets, such as NSL-KDD and UNSW-NB15 [16]. This study ensures a comprehensive benchmarking of these models across various attack scenarios, including DDoS, malware, and reconnaissance. This research aims to bridge critical gaps in cloud security by employing advanced deep learning models to detect and prevent cyber threats proactively. Unlike traditional approaches, these models demonstrate the ability to adapt to evolving threats, reduce false positive rates, and process large-scale, high-dimensional data effectively. The use of LSTM networks, for example, offers superior detection of persistent and complex attack patterns, as evidenced by their highest ROC AUC score of 0.90. Furthermore, the research integrates insights into a practical business model for cloud service providers, offering scalable and adaptive security solutions. These contributions not only enhance the resilience of cloud data centers against diverse cyber threats but also provide actionable guidance for deploying advanced cybersecurity frameworks in real-world applications. By addressing the limitations of traditional methods and exploring the potential of deep learning, this research lays the groundwork for future studies to build hybrid frameworks that combine the strengths of multiple techniques. Real-world testing in diverse cloud environments and optimization strategies to address computational and latency challenges will further refine these solutions, paving the way for next-generation cloud security systems.

II. METHODOLOGY

This study proposes a comprehensive deep learning framework to enhance cloud data center security, leveraging Recurrent Neural Networks (RNNs), Convolutional Neural Networks (CNNs), and Long Short-term Memory (LSTM) networks. The framework integrates anomaly detection and intrusion detection techniques, enabling real-time identification and mitigation of diverse threats. The proposed method integrates statistical and deep learning-based anomaly detection with signature-based and anomaly-based intrusion detection. This multilayered defense mechanism identifies threats early and reduces response time.

A. Data Collection and Preprocessing

Real-time network traffic data from cloud data centers were used. The NSL-KDD and UNSW-NB15 datasets serve as essential resources for studying past network security threats, each offering a unique perspective on historical and modern attack patterns. The NSL-KDD dataset, a refined version of the original KDD Cup 99 dataset, includes network traffic data focusing primarily on traditional cyberattack types from the late 1990s. This dataset is of central importance in IDS research, despite its limitations, such as redundancy in the data processed by NSL-KDD. By improving the quality of the original dataset and removing duplicate records, NSL-KDD provides a powerful tool to evaluate IDS performance in scenarios that reflect past network behaviors and vulnerabilities [17]. On the other hand, the UNSW-NB15 dataset represents more recent advances in cyber threats and modern attack strategies [16]. This dataset was generated in 2015 by simulating network traffic that includes both benign and attack scenarios. It offers a comprehensive set of features and a varied range of attack types, including modern tactics not found in earlier datasets, which makes it particularly useful for training predictive models and enhancing detection systems. The UNSW-NB15 dataset includes a diverse array of network activities and modern attack classes, providing a rich source to understand current and emerging security challenges [17].

The preprocessing steps involved:

- Data cleaning: Duplicate and invalid records were removed from both datasets to ensure consistency and reliability.
- Feature selection: Features with strong correlations to attack patterns were selected through statistical methods, optimizing the model's ability to detect threats.
- Normalization: Numerical features were scaled to the range [0, 1] using min-max scaling to ensure that the data is standardized for model training.
- Sequence padding: Sequences were padded to a consistent length to allow for uniform input into the models, ensuring compatibility with neural networks.
- Data splitting: Datasets were split into 80% for training and 20% for testing using stratified sampling, which preserved the distribution of attack types across the sets.

B. Model Implementation

1) Using CNNs for Feature Extraction

CNNs excel at extracting critical features from data, especially when the data is unstructured or high-dimensional. For instance, in network traffic analysis, CNNs can identify patterns such as sudden traffic spikes or abnormal access behaviors. These capabilities help transform raw data into more interpretable features that can be further analyzed. The objective was to extract relevant features from high-dimensional network traffic data, which can be used to identify unusual behaviors [20].

The input layer used network traffic matrices derived from raw datasets. The model used a convolutional layer with 32 filters, each with a kernel size of 3×3. The Rectified Linear Unit (ReLU) activation function was used to introduce non-linearity and capture complex patterns. A max-pooling layer with a pool size of 2×2 was used to reduce dimensionality while retaining the most important features. Feature maps generated by the pooling layer were processed in the hidden layer to detect patterns in network traffic. Finally, the output layer highlighted traffic patterns, such as spikes or irregular behaviors, potentially indicating a cyberattack.

2) Using LSTM for Predicting Future Patterns or Detecting Attacks

Unlike CNNs, LSTM networks are designed to analyze data in a temporal context. They are highly effective at detecting sequential patterns, such as persistent attack behaviors or gradual anomalies. LSTMs can predict future attacks based on historical data, enhancing early detection capabilities. The objective is to analyze time-series data and predict future attack probabilities or detect emerging threats based on temporal patterns [20]. The input layer uses sequences of network data that represent time-dependent patterns. The hidden layer is an LSTM layer with 128 units designed to capture long-term dependencies in the data. A dropout layer with a rate of 0.2 is used to prevent overfitting by randomly disabling 20% of the neurons during training. LTSM cells utilize the sigmoid and tanh functions to manage the flow of information. The output layer provides predictions of attack likelihoods or classifications of anomalies, aiding in the detection of persistent or evolving threats.

3) Using RNN for Handling Complex and Irregular Sequential Data

RNNs are well-suited for processing irregular or non-periodic data, such as sporadic attacks or unexpected anomalies. By analyzing temporal transitions, RNNs can capture sudden deviations and detect threats that do not follow consistent patterns, making them particularly effective in identifying unpredictable attacks such as malware or sudden DDoS attempts. The objective is to handle unpredictable, sporadic attack patterns that occur irregularly over time [20]. The input layer accepts sequences of time-series data representing unexpected events, such as sudden malware outbreaks or DDoS attacks. The hidden layer consists of one recurrent layer with 128 units using the tanh activation function to capture relationships within sequential data. Finally, the output layer performs the classification of irregular attack patterns, such as bursts of malicious activity, enabling early detection of emergent threats.

C. Hyperparameter Tuning

To optimize model performance, a grid search approach was used to adjust the following hyperparameters.

- The learning rate was tested at values of 0.01, 0.001, and 0.0001, with 0.001 selected for efficient convergence without compromising the model's performance.
- Batch sizes of 16, 32, and 64 were tested, with 32 chosen to balance training speed and model performance in detecting cyberattacks.
- Dropout rates of 0.2, 0.3, and 0.5 were considered, with 0.2 selected to reduce overfitting while maintaining model complexity and effectiveness in detecting attacks.
- The model was trained for 50, 100, and 150 epochs, with 100 epochs selected to ensure adequate training without unnecessary computational time [21].

D. Evaluation Metrics

The following metrics were employed to evaluate the performance of the models. Precision measures the proportion of true positive predictions out of all positive predictions made by the model, reflecting how many of the predicted positive cases were actually correct [18].

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} \quad (1)$$

Recall, also known as sensitivity or the true positive rate, evaluates the model's ability to detect actual positive cases. It shows how well the model identifies true threats [18].

$$\text{Recall} = \frac{\text{TP}}{\text{TP+FN}} \quad (2)$$

The F1 score is the harmonic mean of precision and recall. It provides a balanced evaluation by considering both false positives and false negatives, making it particularly useful for imbalanced datasets where one class significantly outnumbers the other [18].

$$\text{F1} - \text{score} = \frac{2*\text{Precision Recall}}{\text{Precision +Recall}} \quad (3)$$

Accuracy represents the overall correctness of the model by considering both correctly predicted positive and negative cases [18].

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} \quad (4)$$

In these formulas, TP (True Positives) denotes the cases correctly identified as positive (e.g., actual threats detected correctly), TN (True Negatives) denotes the cases correctly identified as negative (e.g., no threat detected when there is none), FP (False Positives) represents the cases incorrectly identified as positive (e.g., benign events flagged as threats), and FN (False Negatives) represent the cases incorrectly identified as negative (e.g., threats missed by the model).

The Receiver Operating Characteristic - Area Under the Curve (ROC-AUC) is a widely accepted performance metric in machine learning and statistics for evaluating the classification accuracy of binary classifiers. It measures the area under the ROC curve, which plots the True Positive Rate (TPR) against the False Positive Rate (FPR) at various classification thresholds [10].

III. RESULTS AND DISCUSSION

The performance of RNN, CNN, and LSTM models was evaluated based on their effectiveness in detecting anomalies and intrusions in network traffic data. Each model processes data differently, leveraging its unique architecture to analyze patterns, identify deviations, and classify network activity. Examining their results using precision, recall, F1 score, accuracy, and ROC-AUC metrics, can highlight their strengths and suitability for cloud data center security.

TABLE I. PERFORMANCE METRICS OF RNN, CNN, AND LSTM MODELS

Model	Precision	Recall	F1 score	Accuracy	ROC-AUC
RNN	0.84	0.87	0.85	0.93	0.89
CNN	0.84	0.82	0.83	0.89	0.89
LSTM	0.82	0.83	0.82	0.89	0.90

The RNN achieved the highest accuracy (93%) and a ROC-AUC score of 0.89, excelling at identifying normal traffic while detecting anomalies with reasonable recall. The CNN demonstrated robust pattern recognition with a balanced performance (accuracy: 89%, ROC-AUC: 0.89). CNN is suitable for rapid and real-time intrusion detection. The LSTM model attained the highest ROC AUC score (0.90), indicating a superior ability to distinguish between normal and anomalous traffic. LSTM's performance balances recall and precision effectively.

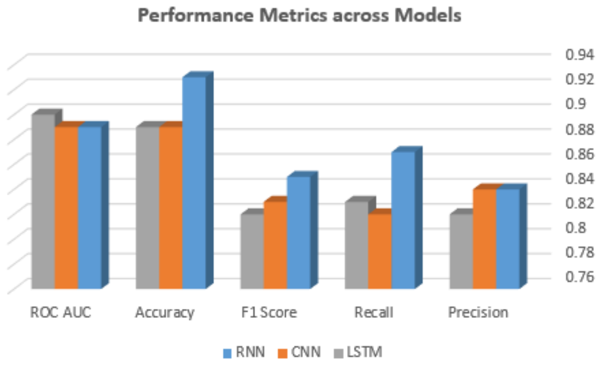

Fig. 1. Performance metrics across models.

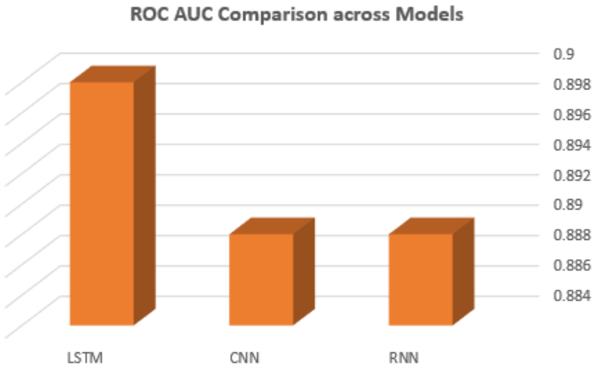

Fig. 2. ROC-AUC comparison across models.

Figure 2 illustrates the ROC-AUC performance of the RNN, CNN, and LSTM models. The ROC-AUC score reflects the models' ability to distinguish between classes effectively, with higher values indicating better performance. The results of these models demonstrate their distinct strengths and weaknesses in detecting anomalies and intrusions in cloud data center environments.

The RNN model achieved an accuracy of 93% with a ROC AUC score of 0.89. These metrics reflect its strong ability to handle sequential data, making it effective for detecting patterns in time-series datasets. However, the model's relatively lower precision (0.71) for anomalies indicates a tendency for false positives, which may limit its utility in environments where precision is critical.

The CNN model achieved an overall accuracy of 89% and a ROC-AUC score of 0.89, indicating its reliability for real-time intrusion detection. Its ability to process high-dimensional data efficiently makes it suitable for immediate threat detection, such as DDoS attacks. However, the slightly lower recall for anomalies (0.70) suggests that it may miss some anomalous activities, necessitating careful consideration for deployment in high-security environments.

The LSTM model stands out with the highest ROC-AUC score of 0.90, demonstrating its superior ability to capture long-term dependencies in the data. This makes it particularly effective for detecting persistent threats, such as insider attacks, that require an understanding of temporal patterns over extended periods. However, its computational intensity and latency challenges must be addressed for real-time deployment.

IV. CONCLUSION

This study addresses the critical challenge of real-time anomaly detection and intrusion prevention in cloud data centers using deep learning techniques. A comprehensive evaluation of RNN, CNN, and LSTM models was conducted, yielding significant findings that contribute to the advancement of cloud security. Among these models, RNN achieved the highest recall (0.87) and F1 score (0.85), making it highly effective in identifying true positive cases. CNN demonstrated competitive performance, with a precision of 0.84 and a ROC-AUC of 0.89, displaying its ability to process complex attack patterns. Meanwhile, the LSTM model, despite a slightly lower F1 score and recall, achieved the highest ROC AUC score of 0.90, indicating superior performance in distinguishing between normal and anomalous traffic. This research fills a knowledge gap by offering an in-depth analysis of these models within the context of high-dimensional, dynamic data prevalent in cloud environments. Unlike previous studies, which often focused on isolated datasets or lacked scalability evaluations, this work integrates the NSL-KDD and UNSW-NB15 datasets to provide a robust and generalizable solution. The proposed models not only improve detection accuracy (up to 93% for RNN) but also demonstrate their potential for deployment in real-time environments, surpassing traditional approaches that fail to address dynamic attack patterns effectively.

Compared to previous studies, which achieved lower ROC AUC scores, LSTM's performance underscores its robustness in handling evolving cyber threats. A major contribution of this research is the establishment of a foundation for hybrid frameworks to combine the strengths of multiple deep learning models to achieve higher adaptability and efficiency. Future research will focus on further optimizing these models, conducting large-scale real-world validations, and integrating reinforcement learning to enhance adaptability and decision-making under changing threat conditions.

REFERENCES

[1] "Cost of a data breach 2023," *IBM*. https://www.ibm.com/reports/data-breach.

[2] S. G. Kene and D. P. Theng, "A review on intrusion detection techniques for cloud computing and security challenges," in *2015 2nd International Conference on Electronics and Communication Systems (ICECS)*, Coimbatore, India, Feb. 2015, pp. 227–232, https://doi.org/10.1109/ECS.2015.7124898.

[3] L. Abrams, "Over 500,000 Zoom accounts sold on hacker forums, the dark web," *BleepingComputer*. https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/.

[4] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Computing Surveys*, vol. 41, no. 3, Apr. 2009, https://doi.org/10.1145/1541880.1541882.

[5] I. Ahmad, M. Basheri, M. J. Iqbal, and A. Rahim, "Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection," *IEEE Access*, vol. 6, pp. 33789–33795, 2018, https://doi.org/10.1109/ACCESS.2018.2841987.

[6] Z. Chkirbene, A. Erbad, R. Hamila, A. Gouissem, A. Mohamed, and M. Hamdi, "Machine Learning Based Cloud Computing Anomalies Detection," *IEEE Network*, vol. 34, no. 6, pp. 178–183, Nov. 2020, https://doi.org/10.1109/MNET.011.2000097.

[7] S. Rahman, S. Pal, S. Mittal, T. Chawla, and C. Karmakar, "SYN-GAN: A robust intrusion detection system using GAN-based synthetic data for IoT security," *Internet of Things*, vol. 26, Jul. 2024, Art. no. 101212, https://doi.org/10.1016/j.iot.2024.101212.

[8] B. Mopuru and Y. Pachipala, "Enhanced Intrusion Detection in IoT with a Novel PRBF Kernel and Cloud Integration," *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 14988–14993, Aug. 2024, https://doi.org/10.48084/etasr.7767.

[9] A. A. Alhashmi, A. A. Darem, A. B. Alshammari, L. A. Darem, H. K. Sheatah, and R. Effghi, "Ransomware Early Detection Techniques," *Engineering, Technology & Applied Science Research*, vol. 14, no. 3, pp. 14497–14503, Jun. 2024, https://doi.org/10.48084/etasr.6915.

[10] S. Ahmad, A. Lavin, S. Purdy, and Z. Agha, "Unsupervised real-time anomaly detection for streaming data," *Neurocomputing*, vol. 262, pp. 134–147, Nov. 2017, https://doi.org/10.1016/j.neucom.2017.04.070.

[11] J. B. Awotunde, C. Chakraborty, and A. E. Adeniyi, "Intrusion Detection in Industrial Internet of Things Network-Based on Deep Learning Model

with Rule-Based Feature Selection," *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, 2021, Art. no. 7154587, https://doi.org/10.1155/2021/7154587.

[12] T. A. Devi and A. Jain, "Enhancing Cloud Security with Deep Learning-Based Intrusion Detection in Cloud Computing Environments," in *2024 2nd International Conference on Advancement in Computation &amp; Computer Technologies (InCACCT)*, Gharuan, India, May 2024, pp. 541–546, https://doi.org/10.1109/InCACCT61598.2024.10551040.

[13] I. Ullah and Q. H. Mahmoud, "Design and Development of RNN Anomaly Detection Model for IoT Networks," *IEEE Access*, vol. 10, pp. 62722–62750, 2022, https://doi.org/10.1109/ACCESS.2022.3176317.

[14] B. Lindemann, B. Maschler, N. Sahlab, and M. Weyrich, "A survey on anomaly detection for technical systems using LSTM networks," *Computers in Industry*, vol. 131, Oct. 2021, Art. no. 103498, https://doi.org/10.1016/j.compind.2021.103498.

[15] L. Mohammadpour, T. C. Ling, C. S. Liew, and A. Aryanfar, "A Survey of CNN-Based Network Intrusion Detection," *Applied Sciences*, vol. 12, no. 16, Jan. 2022, Art. no. 8162, https://doi.org/10.3390/app12168162.

[16] M. Nour and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *2015 Military Communications and Information Systems Conference (MilCIS)*, Canberra, Australia, Nov. 2015, pp. 1–6, https://doi.org/10.1109/MilCIS.2015.7348942.

[17] M. S. Al-Daweri, K. A. Zainol Ariffin, S. Abdullah, and M. F. E. Md. Senan, "An Analysis of the KDD99 and UNSW-NB15 Datasets for the Intrusion Detection System," *Symmetry*, vol. 12, no. 10, p. 1666, Oct. 2020, https://doi.org/10.3390/sym12101666.

[18] D. M. W. Powers, "Evaluation: from precision, recall and F-measure to ROC, informedness, markedness and correlation." arXiv, Oct. 11, 2020, https://doi.org/10.48550/arXiv.2010.16061.

[19] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, Ottawa, ON, Canada, Jul. 2009, pp. 1–6, https://doi.org/10.1109/CISDA.2009.5356528.

[20] F. M. Shiri, T. Perumal, N. Mustapha, and R. Mohamed, "A Comprehensive Overview and Comparative Analysis on Deep Learning Models: CNN, RNN, LSTM, GRU." arXiv, Oct. 24, 2024, https://doi.org/10.48550/arXiv.2305.17473.

[21] J. Brownlee, "How to Grid Search Hyperparameters for Deep Learning Models in Python with Keras," *MachineLearningMastery.com*, 2022. https://www.machinelearningmastery.com/grid-search-hyperparameters-deep-learning-models-python-keras/.