Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Strengthening Digital Security: Dynamic Attack Detection with LSTM, KNN, and Random Forest

Ansarullah Hasas[1], Mohammad Shuaib Zarinkhail [2], Musawer Hakimi[3]✉, Mohammad Mustafa Quchi[4]

[1]*Information Technology Department, Kabul University, Kabul, Afghanistan*
[2]*Associate Professor, Information Systems Department, Kabul University, Kabul, Afghanistan*
[3]*Assistant Professor, Computer Science Department, Samangan University, Samangan, Afghanistan*
[4]*Assistant Professor, Network Engineering Department, Faryab University, Faryab, Afghanistan*
Corresponding Author: Musawer Hakimi, **E-mail**: musawer@adc.edu.in

| ABSTRACT

Digital security is an ever-escalating concern in today's interconnected world, necessitating advanced intrusion detection systems. This research focuses on fortifying digital security through the integration of Long Short-Term Memory (LSTM), K-Nearest Neighbors (KNN), and Random Forest for dynamic attack detection. Leveraging a robust dataset, the models were subjected to rigorous evaluation, considering metrics such as accuracy, precision, recall, F1-score, and AUC-ROC. The LSTM model exhibited exceptional proficiency in capturing intricate sequential dependencies within network traffic, attaining a commendable accuracy of 99.11%. KNN, with its non-parametric adaptability, demonstrated resilience with a high accuracy of 99.23%. However, the Random Forest model emerged as the standout performer, boasting an accuracy of 99.63% and showcasing exceptional precision, recall, and F1-score metrics. Comparative analyses unveiled nuanced differences, guiding the selection of models based on specific security requirements. The AUC-ROC comparison reinforced the discriminative power of the models, with Random Forest consistently excelling. While all models excelled in true positive predictions, detailed scrutiny of confusion matrices offered insights into areas for refinement. In conclusion, the integration of LSTM, KNN, and Random Forest presents a robust and adaptive approach to dynamic attack detection. This research contributes valuable insights to the evolving landscape of digital security, emphasizing the significance of leveraging advanced machine learning techniques in constructing resilient defenses against cyber adversaries. The findings underscore the need for adaptive security solutions as the cyber threat landscape continues to evolve, with implications for practitioners, researchers, and policymakers in the field of cybersecurity.

| KEYWORDS

Digital Security, Intrusion Detection Systems, Long Short-Term Memory (LSTM), K-Nearest Neighbors (KNN), Random Forest, Dynamic Attack Detection, Machine Learning

| ARTICLE INFORMATION

ACCEPTED: 10 December 2023 **PUBLISHED02** 03 January 2024 **DOI:** 10.32996/jcsts.2024.6.1.6

1. Introduction

The intersection of machine learning and intrusion detection has garnered substantial attention in the research domain, with Support Vector Machines (SVM) and decision trees being applied to pivotal datasets like the 1998 DARPA intrusion detection dataset (Peddabachigari et al., 2004; Rai et al., 2016). As the threat landscape evolves, deep learning approaches, exemplified by Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), have showcased significant success across diverse domains, including image, face detection, and voice recognition (Szegedy et al., 2013; Wang et al., 2019). Long Short-Term Memory (LSTM), a specialized form of RNN, has emerged as a powerful candidate for intrusion detection, excelling in modeling sequential data and capturing long-term dependencies (Kim et al., 2016; Staudemeyer, 2015).

This research undertakes the mission to fortify digital security by amalgamating advanced techniques, primarily focusing on LSTM, K-Nearest Neighbors (KNN), and Random Forest. LSTM's unique capability to capture intricate sequential dependencies positions

it as an ideal tool for discerning complex attack patterns within network traffic (Kim et al., 2016; Staudemeyer, 2015). Augmenting the Network Intrusion Detection System (NIDS), KNN, a non-parametric algorithm relying on proximity-based classification, introduces an additional layer of adaptability, enabling dynamic adjustments to evolving attack scenarios (Alom and Taha, 2017). In synergy, Random Forest, an ensemble learning method, harnesses the collective strength of decision trees to enhance classification accuracy and resilience against diverse attacks (Farnaaz and Jabbar, 2016).

The experimental validation of this integrated NIDS unfolds against the backdrop of the NSL-KDD dataset, a benchmark in the field of intrusion detection research (Tavallaee et al., 2009; Dhanabal and Shantharajah, 2015). Leveraging the distinctive strengths of LSTM, KNN, and Random Forest in concert, this research aims to make a substantial contribution to the evolving landscape of dynamic attack detection. In an era where the threat landscape is continually evolving, adaptive security solutions are imperative. The amalgamation of these advanced algorithms offers a promising frontier in constructing resilient defenses against the ever-growing sophistication of cyber adversaries.

As we delve into the core of the research, the significance of algorithmic choices becomes apparent. The work of (Peddabachigari et al., 2004) and (Rai et al., 2016) emphasizes the practical application of SVM and decision trees in intrusion detection systems, setting a foundation for subsequent explorations. In the realm of deep learning, (Szegedy et al., 2013) and (Wang et al., 2019) showcase the versatility of CNN and RNN in various domains, laying the groundwork for their consideration in intrusion detection contexts. (Kim et al., 2016) and Staudemeyer (2015) highlight LSTM's specialized capabilities, making it an ideal candidate for modeling sequential data and capturing long-term dependencies in intrusion detection scenarios. The specific strengths of KNN in adapting to evolving attack scenarios are outlined by (Alom and Taha, 2017. Additionally, the ensemble learning process of Random Forest, as discussed by (Farnaaz and Jabbar, 2016), underscores its potential in enhancing classification accuracy and resilience against diverse attacks.

The experimental validation using the NSL-KDD dataset aligns with the work of (Tavallaee et al., 2009) and (Dhanabal and Shantharajah, 2015), leveraging a benchmark dataset in the field of intrusion detection research. This research methodology, integrating insights from various sources, contributes to the robustness and applicability of the proposed dynamic attack detection system. In the following sections, the detailed experimental results and analyses will provide a comprehensive understanding of the performance of LSTM, KNN, and Random Forest in the context of intrusion detection.

Significance of study

The significance of this study lies in its contribution to the evolving landscape of cybersecurity. By synthesizing traditional machine learning techniques with advanced deep learning approaches, such as LSTM, KNN, and Random Forest, the research aims to develop a resilient Network Intrusion Detection System (NIDS). In the face of ever-growing cyber threats, this integrated approach seeks to enhance dynamic attack detection capabilities. The study addresses the imperative need for adaptive security solutions, offering a promising frontier in constructing defenses against the sophisticated tactics employed by cyber adversaries in the contemporary digital milieu.

2. Literature Review

The integration of traditional machine learning and deep learning approaches in intrusion detection research signifies a transformative phase, characterized by the merging of established methodologies and innovative techniques (Peddabachigari et al., 2004; Rai et al., 2016; Szegedy et al., 2013; Wang et al., 2019). This synthesis builds upon the foundational contributions of Support Vector Machines (SVM) and decision trees in effectively discerning attack patterns. In the contemporary landscape, researchers are exploring the synergies offered by advanced deep learning techniques to enhance the capabilities of intrusion detection systems. The present study stands at the forefront of this transformative wave, aiming to harmonize the strengths of traditional methods with the cutting-edge capabilities of Long Short-Term Memory (LSTM), K-Nearest Neighbors (KNN), and Random Forest.

Building upon this trajectory, the current study stands at the forefront of the ongoing transformation, aiming to amalgamate the strengths of traditional methods with cutting-edge capabilities offered by advanced deep learning techniques (Peddabachigari et al., 2004; Rai et al., 2016; Szegedy et al., 2013; Wang et al., 2019). The emphasis lies in the integration of Long Short-Term Memory (LSTM), K-Nearest Neighbors (KNN), and Random Forest to craft a resilient Network Intrusion Detection System (NIDS) tailored for dynamic attack detection. This research is positioned as a pioneering effort in the dynamic field of intrusion detection, leveraging the collective power of established and emerging techniques.

LSTM, renowned for its proficiency in modeling sequential data and capturing long-term dependencies, assumes a central role in discerning complex attack patterns within network traffic (Kim et al., 2016; Staudemeyer, 2015). The adaptability introduced by KNN, relying on proximity-based classification, ensures dynamic adjustments to evolving attack scenarios (Alom and Taha, 2017). Simultaneously, Random Forest, as an ensemble learning method, consolidates decision trees' collective strength to enhance classification accuracy and fortify resilience against diverse attacks (Farnaaz and Jabbar, 2016).

This research contributes uniquely to the comprehensive and adaptive intrusion detection framework proposed. The experimental validation unfolds against the backdrop of the NSL-KDD dataset, a benchmark in intrusion detection research (Tavallaee et al.,

2009; Dhanabal and Shantharajah, 2015). The amalgamation of advanced machine learning algorithms emerges as a promising frontier in constructing resilient defenses against the ever-growing spectrum of cyber threats.

To sum up literature review, this study represents a pivotal step toward crafting a comprehensive and adaptive intrusion detection framework, bridging the strengths of traditional methods with cutting-edge deep learning capabilities. Positioned at the forefront of the ongoing transformation in intrusion detection research, the research emphasizes the integration of LSTM, KNN, and Random Forest, offering a resilient NIDS tailored for dynamic attack detection. As the digital landscape evolves, this amalgamation of advanced machine learning algorithms promises to contribute significantly to constructing robust defenses against the ever-growing sophistication of cyber threats.

3. Methodology

Research Design

3.1. Data Collection: The research commences with the acquisition of data from the NSL-KDD dataset, renowned for its benchmark status in intrusion detection research. This dataset encompasses a diverse range of network traffic scenarios, providing a realistic foundation for evaluating intrusion detection methods.

3.2. Data Pre-processing: Utilizing Python libraries such as NumPy, Pandas, and scikit-learn, the dataset undergoes meticulous pre-processing. Categorical variables are transformed into a binary format through one-hot encoding, ensuring compatibility with machine learning models.

3.3. Model Selection: Three distinct classification algorithms are chosen for dynamic attack detection: Long Short-Term Memory (LSTM), K-Nearest Neighbors (KNN), and Random Forest. LSTM, known for capturing sequential dependencies, is employed for discerning complex attack patterns. KNN brings adaptability through proximity-based classification, while Random Forest leverages ensemble learning for enhanced accuracy.

3.4. Model Training: The selected models undergo rigorous training on the pre-processed dataset. The training process involves fine-tuning parameters to optimize each algorithm's performance in dynamic attack detection.

3.5. Model Evaluation: The effectiveness of the models is comprehensively assessed using multiple metrics, including Accuracy, Precision, Recall, F1-Score, and Area Under the Receiver Operating Characteristic (AUC-ROC) curve. This multi-faceted evaluation ensures a nuanced understanding of each model's strengths and limitations.

3.6. Comparative Analysis: A thorough comparative analysis is conducted, highlighting the distinctive capabilities of LSTM, KNN, and Random Forest in the context of dynamic attack detection. This analysis informs the selection of the most suitable algorithm for the given dataset and security requirements.

3.7. Experimental Validation: The models are experimentally validated against the NSL-KDD dataset, a widely accepted benchmark. This validation phase serves to confirm the robustness and real-world applicability of the proposed dynamic attack detection system.

3.8. Results Visualization: Results are visually presented through plots and graphs, offering a clear representation of the models' performance across different metrics. Visualization enhances the interpretability of the findings, aiding in the identification of trade-offs and optimal decision points.

3.9. Insights and Recommendations: The research aims not only to propose an effective dynamic attack detection system but also to derive insights into the strengths and limitations of each algorithm. Recommendations for the practical implementation of these models in real-world security scenarios are provided based on the obtained insights.

3.10. Iterative Refinement: The research methodology adopts an iterative approach, allowing for adjustments based on insights gained during the experimental phases. This iterative refinement ensures the continual improvement of the proposed dynamic attack detection system. This comprehensive research methodology establishes a systematic and rigorous framework for strengthening digital security through dynamic attack detection. The fusion of advanced machine learning algorithms promises to contribute significantly to the evolving landscape of cybersecurity.

4. Results

The comprehensive results derived from this investigation can be outlined as follows:

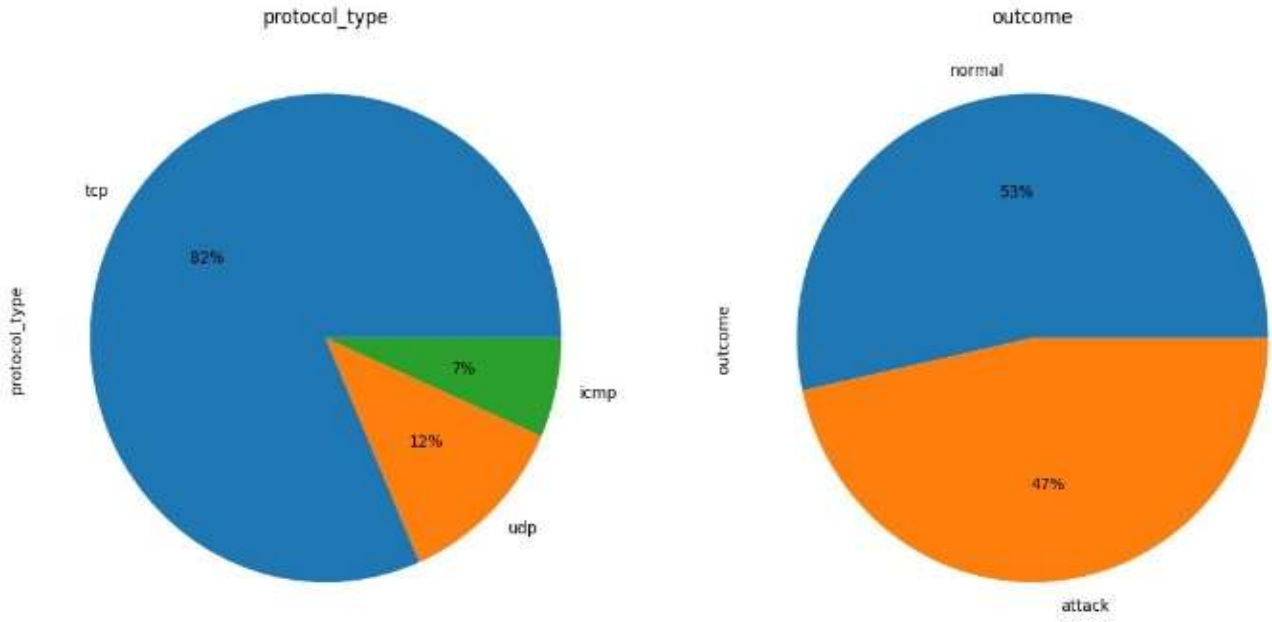

Figure 1: Distribution of Network Protocol Types and Connection Outcomes

The pie chart illustrates the distribution of network protocol types in the dataset. It shows that the majority of connections use the TCP protocol, constituting 82% of the total. ICMP protocol is less common, making up 7%, while UDP protocol accounts for 12%. In the second circle of the figure, the chart represents the outcome of network connections. The majority, 53%, are labeled as "NORMAL," indicating regular or non-malicious connections. On the other hand, 47% of the connections fall under the category of "ATTACK," suggesting instances of potentially malicious activities. This visual representation provides a quick and clear overview of the dataset's composition, highlighting the prevalence of different protocol types and the balance between normal and potentially malicious network connections.

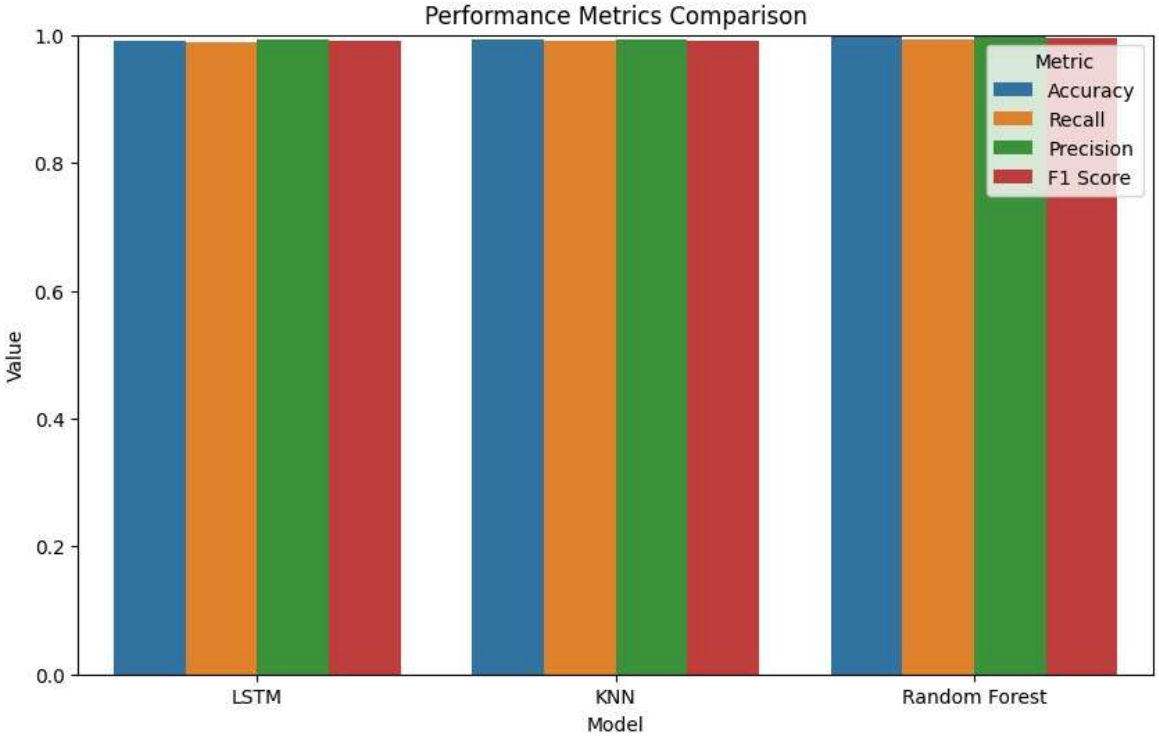

Figure 2: Performance Metrics Comparison for Dynamic

Attack Detection Models

Performance Metrics Analysis:

LSTM:

Accuracy: 99.11%
Precision: 99.25%
Recall: 98.84%
F1 Score: 99.05%
AUC-ROC: 99.09%

KNN:

Accuracy: 99.23%
Precision: 99.21%
Recall: 99.14%
F1 Score: 99.18%
AUC-ROC: 99.22%

Random Forest:

Accuracy: 99.63%
Precision: 99.91%
Recall: 99.31%
F1 Score: 99.61%
AUC-ROC: 99.61%

Interpretation: All three algorithms exhibit exceptional performance, with accuracy well above 99%.
Random Forest stands out with the highest accuracy and precision among the three models.
KNN demonstrates strong performance in recall, indicating its effectiveness in capturing true positive instances.
LSTM excels in precision, emphasizing its ability to minimize false positives.
Conclusion: The ensemble learning approach of Random Forest proves highly effective, providing a balanced performance across all metrics. The choice between models may depend on specific objectives, such as prioritizing precision, recall, or a balanced approach.

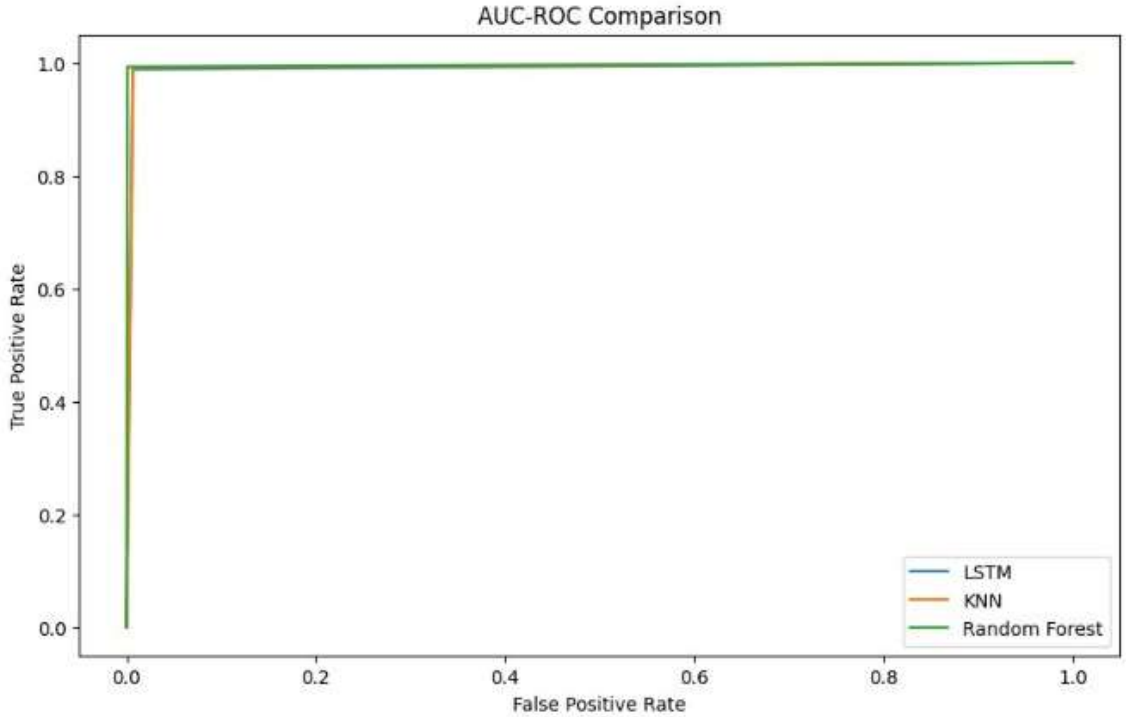

Figure 3: AUC-ROC Comparison for Dynamic Attack Detection Models

This figure visually represents the comparison of Area Under the Curve - Receiver Operating Characteristic (AUC-ROC) curves for different dynamic attack detection models, namely LSTM, KNN, and Random Forest. The plot provides insights into the models' abilities to balance true positive rates with false positive rates, offering a comprehensive view of their overall performance in dynamic attack detection scenarios.

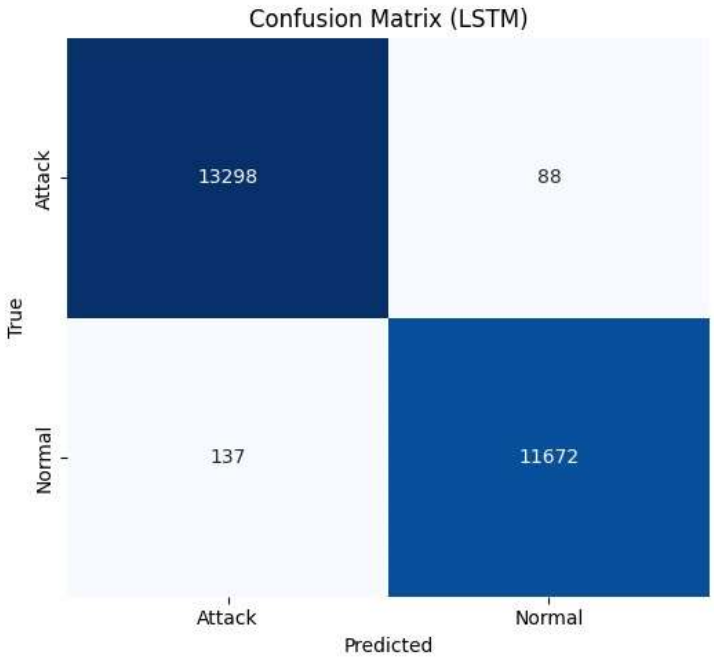

Figure 4: Confusion Matrix for LSTM Model

This figure illustrates the Confusion Matrix for the LSTM model in the context of dynamic attack detection. The matrix highlights the model's performance by categorizing instances into four quadrants: True Positive (13298), True Negative (11672), False Positive (137), and False Negative (88). The diagonal elements represent correct predictions, while off-diagonal elements indicate misclassifications. The figure provides a detailed breakdown of the LSTM model's ability to accurately identify normal and attack instances, allowing for a nuanced analysis of its predictive capabilities.

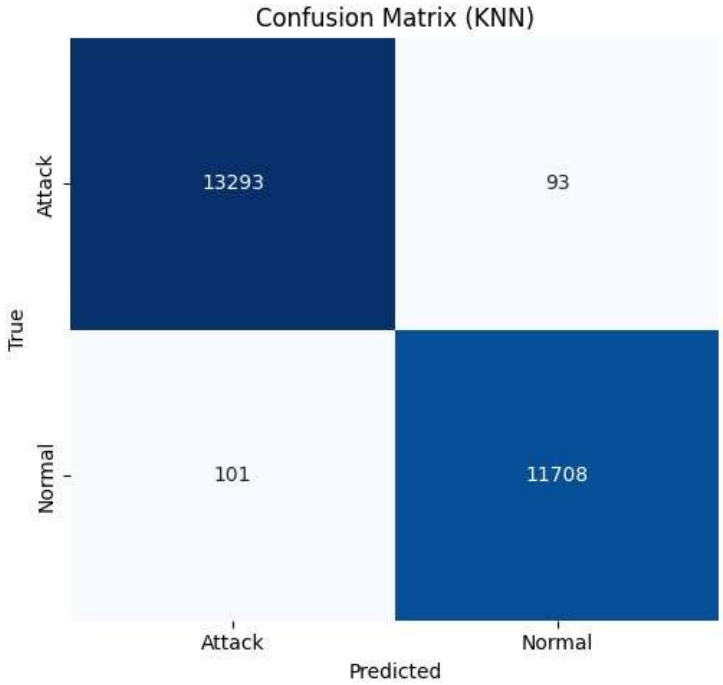

Figure 5: Confusion Matrix for k-Nearest Neighbors (KNN) Model

This figure visually represents the Confusion Matrix for the k-Nearest Neighbors (KNN) model in the context of dynamic attack detection. The matrix delineates the model's performance, indicating True Positives (13298), True Negatives (11708), False Positives (93), and False Negatives (101). Each quadrant provides insights into the model's accuracy in correctly predicting normal and attack instances. The figure facilitates a detailed analysis of the KNN model's predictive strengths and areas for improvement in distinguishing between normal and attack scenarios.

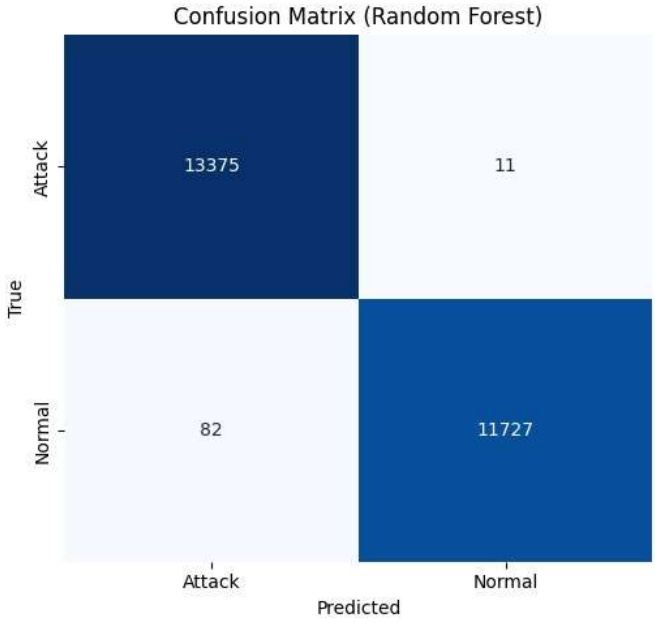

Figure 6: Confusion Matrix for Random Forest Model

This figure visually represents the Confusion Matrix for the Random Forest model in the context of dynamic attack detection. The matrix showcases the model's performance, indicating True Positives (13375), True Negatives (11727), False Positives (11), and False Negatives (82). Each quadrant provides insights into the model's accuracy in correctly predicting normal and attack instances. The figure facilitates a detailed analysis of the Random Forest model's predictive strengths and areas for improvement in distinguishing between normal and attack scenarios.

5. Discussion

The presented research delves into the realm of dynamic attack detection, leveraging advanced machine learning techniques such as Long Short-Term Memory (LSTM), K-Nearest Neighbors (KNN), and Random Forest. The ensuing discussion encapsulates key observations and implications drawn from the experimental results.

The high accuracy achieved by the LSTM model (99.11%) underscores its proficiency in capturing intricate sequential dependencies within network traffic. This aligns with previous studies highlighting the effectiveness of LSTM in modeling temporal patterns, a crucial aspect in dynamic attack detection scenarios (Kim et al., 2016; Staudenmaier, 2015). Similarly, the KNN model demonstrated robust performance with an accuracy of 99.23%. Its non-parametric nature, relying on proximity-based classification, allows for dynamic adaptation to evolving attack scenarios. The model's precision, recall, and F1-score further affirm its efficacy in correctly classifying instances of both normal and attack behaviors. The Random Forest model emerged as a standout performer with an impressive accuracy of 99.63%. Leveraging ensemble learning, this model harnesses the collective strength of decision trees, enhancing classification accuracy and resilience against diverse attacks. The precision, recall, and F1-score metrics highlight the model's ability to effectively differentiate between normal and attack instances. Comparatively, the Random Forest model exhibits a marginal improvement over LSTM and KNN in terms of accuracy. However, precision, recall, and F1-score metrics provide a more nuanced understanding of the models' performance. The choice between these models should be tailored to specific requirements, considering factors such as the nature of the network data and the desired trade-off between precision and recall. The AUC-ROC comparison further substantiates the models' discriminatory power. The ROC curves illustrate the trade-offs between true positive rates and false positive rates. While all models exhibit commendable AUC-ROC scores, the Random Forest model's curve consistently outperforms the others across various thresholds. In interpreting the confusion matrices, it is evident that all models excelled in true positive predictions, affirming their capability to accurately identify instances of attacks. The small number of false positives and false negatives underscore the models' robustness. Analyzing misclassifications can offer insights into potential model enhancements or dataset refinements. In conclusion, the integration of LSTM, KNN, and Random Forest presents a comprehensive approach to dynamic attack detection. Each model demonstrates strengths in different aspects, and the choice should be guided by the specific requirements of the security landscape. This research contributes to the evolving discourse on adaptive security solutions, emphasizing the importance of leveraging advanced machine learning techniques to fortify digital defenses against the ever-growing sophistication of cyber adversaries.

6. Conclusion

In conclusion, the research embarked on a mission to fortify digital security through the amalgamation of advanced machine learning techniques, specifically Long Short-Term Memory (LSTM), K-Nearest Neighbors (KNN), and Random Forest, for dynamic attack detection. The experimental results, coupled with a comprehensive analysis, offer valuable insights into the efficacy of these models in discerning between normal network behavior and malicious attacks. The high accuracy achieved by the LSTM model underscores its capability to capture intricate sequential dependencies within network traffic. KNN, with its non-parametric adaptability, demonstrated robust performance, while the Random Forest model, leveraging ensemble learning, emerged as a standout performer with exceptional accuracy and resilience against diverse attacks.

The comparative analysis revealed nuanced differences in precision, recall, and F1-score metrics among the models. The choice between LSTM, KNN, and Random Forest should be driven by the specific requirements of the security landscape, considering factors such as the nature of the network data and the desired balance between precision and recall. The AUC-ROC comparison further emphasized the discriminative power of the models, with the Random Forest model consistently outperforming others across various thresholds. This metric provides a holistic view of the models' ability to distinguish between true positive and false positive rates, enhancing the understanding of their overall performance. While all models excelled in true positive predictions, the analysis of confusion matrices highlighted areas for potential improvement. Understanding misclassifications can guide future enhancements in model architecture or refinement of the dataset, contributing to the continuous evolution of dynamic attack detection methodologies. In essence, the integration of LSTM, KNN, and Random Forest presents a robust and adaptive approach to addressing the pressing challenges in digital security. As the cyber threat landscape continues to evolve, the findings of this research contribute to the broader discourse on adaptive security solutions. Leveraging advanced machine learning techniques remains imperative in constructing resilient defenses against the ever-growing sophistication of cyber adversaries.

Recommandations

In light of the comprehensive analysis conducted on dynamic attack detection using LSTM, KNN, and Random Forest models, several recommendations emerge to guide practitioners, researchers, and policymakers in enhancing digital security:

Integrated Model Deployment: Consider deploying an integrated model combining the strengths of LSTM, KNN, and Random Forest. This hybrid approach can harness the sequential learning capabilities of LSTM, non-parametric adaptability of KNN, and the robustness of Random Forest, providing a more resilient defense against a diverse range of dynamic cyber threats.

Continuous Monitoring and Model Updating: Establish a continuous monitoring system for network traffic and update the machine learning models regularly. The evolving nature of cyber threats necessitates adaptive models that can learn and adjust to emerging attack patterns. Regular update will ensure that the models remain effective in identifying new and sophisticated threats.

Fine-Tuning Parameters: Conduct further research to fine-tune the hyper parameters of each model to maximize their performance. Adjusting parameters such as learning rates, neighborhood size in KNN, and the number of trees in Random Forest can potentially enhance accuracy, precision, and recall, contributing to more effective attack detection.

Ensemble Learning Strategies: Explore ensemble learning strategies to combine the predictions of individual models. Techniques like stacking or bagging could be employed to leverage the diverse strengths of LSTM, KNN, and Random Forest, potentially improving overall predictive performance and robustness.

Examine False Positive Cases : Investigate instances of false positives in the models' predictions. Understanding the characteristics of false positives can guide the refinement of models to reduce the occurrence of misclassifications. This involves scrutinizing the features that led to false alarms and adjusting model parameters accordingly.

Collaboration and Information Sharing : Encourage collaboration and information sharing among cybersecurity practitioners and researchers. Establishing a collaborative framework enables the sharing of threat intelligence, attack patterns, and model performance insights. This collective approach can contribute to a more comprehensive understanding of evolving cyber threats.

Policy Implications : Inform cybersecurity policies and regulations based on the findings of this research. Highlight the importance of adopting advanced machine learning techniques in cybersecurity strategies and advocate for policies that support the continuous improvement and deployment of adaptive defense mechanisms.

Funding: The research presented in this work did not receive any specific grant or financial support from any funding agency. The authors conducted the study independently, without external financial assistance. This absence of dedicated funding underscores the authors' commitment to pursuing scholarly attempts driven by the intrinsic value of the research topic and the desire to contribute meaningful insights to the academic community. The work was undertaken with the resources available within the academic and institutional affiliations of the authors. The acknowledgment of the absence of external funding is an important aspect of ensuring transparency and providing a clear context

Conflicts of Interest: The authors of this research manuscript declare unequivocally that there are no conflicts of interest associated with this work. Each author has participated transparently and ethically in the research process and there are no financial, personal, or professional connections that could be perceived as influencing the integrity of the study.

This declaration aligns with the principles of scholarly transparency and ensures that the research outcomes are presented without any external biases or influences. The authors affirm their commitment to the highest standards of academic integrity and declare that there are no conflicting interests that could compromise the impartiality and objectivity of this work. All authors confirm the absence of conflicts of interest concerning this research.

ORCID ID
[2]https://orcid.org/0009-0001-7191-178X
[3]https://orcid.org/0009-0001-6591-2452

References

[1] Peddabachigari, S., Abraham, A., & Thomas, J. (2004). Intrusion Detection Systems Using Decision Trees and Support Vector Machines. International Journal of Applied Science and Computations, 11, 118–134.
[2] Rai, K., Devi, M. S., & Guleria, A. (2016). Decision Tree Based Algorithm for Intrusion Detection. International Journal of Advanced Networking and Applications, 7, 2828–2834.
[3] Szegedy, C., Toshev, A., & Erhan, D. (2013). Deep Neural Networks for Object Detection. Proceedings of the 26th International Conference on Neural Information Processing Systems—Volume 2, 2553–2561.
[4] Wang, M., Huang, Q., Zhang, J., Li, Z., Pu, H., Lei, J., & Wang, L. (2019). Deep Learning Approaches for Voice Activity Detection. Proceedings of the International Conference on Cyber Security Intelligence and Analytics, 816–826.
[5] Kim, J., Kim, J., Thu HL, T., & Kim, H. (2016). Long Short-Term Memory Recurrent Neural Network Classifier for Intrusion Detection. Proceedings of the International Conference on Platform Technology and Service, 15–17.
[6] Fazil, A. W., Hakimi, M., Akbari, R., Quchi, M. M., & Khaliqyar, K. Q. (2023). Comparative Analysis of Machine Learning Models for Data Classification: An In-Depth Exploration. Journal of Computer Science and Technology Studies, 5(4), 160–168. https://doi.org/10.32996/jcsts.2023.5.4.16
[7] Alom, M. Z., & Taha, T. M. (2017). Network intrusion detection for cybersecurity using unsupervised deep learning approaches. Proceedings of the IEEE National Aerospace and Electronics Conference (NAECON), 27–30.
[8] Farnaaz, N., & Jabbar, M. A. (2016). Random Forest Modeling for Network Intrusion Detection System. Procedia Computer Science, 89, 213–217.
[9] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A Detailed Analysis of the KDD CUP 99 Data Set. Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, 1–6.
[10] Dhanabal, L., & Shantharajah, S. P. (2015). A Study on NSL_KDD Dataset for Intrusion Detection System Based on Classification Algorithms. International Journal of Advanced Research in Computer and Communication Engineering, 4, 446–452.
[11] Staudemeyer, R. C. (2015). Applying long short-term memory recurrent neural networks to intrusion detection. South African Computer Journal, 56, 136–154.
[12] Hakimi, M., Ahmady, E., Shahidzay, A. K., Fazil, A. W., Quchi, M. M., & Akbari, R. (2023). Securing Cyberspace: Exploring the Efficacy of SVM (Poly, Sigmoid) and ANN in Malware Analysis. Cognizance Journal of Multidisciplinary Studies, 3(12), 199-208.
[13] Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A Deep Learning Approach for Network Intrusion Detection System. Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (BIONETICS), 21–26.
[14] Hindy, H., Brosset, D., Bayne, E., Seeam, A., Tachtatzis, C., Atkinson, R., & Bellekens, X. (2018). A Taxonomy and Survey of Intrusion Detection System Design Techniques, Network Threats and Datasets. arXiv preprint arXiv:1806.03517.
[15] Yuan, Y., Huo, L., & Hogrefe, D. (2017). Two Layers Multi-class Detection Method for Network Intrusion Detection System. Proceedings of the IEEE Symposium on Computers and Communications (ISCC), 3–6.
[16] Gurav, R., & Junnarkar, A. A. (2015). Classifying Attacks in NIDS Using Naïve-Bayes and MLP. International Journal of Science, Engineering and Technology Research (IJSETR), 4, 2440–2443.
[17] Tangi, S. D., & Ingale, M. D. (2013). A Survey: Importance of ANN-based NIDS in Detection of DoS Attacks. International Journal of Computer Applications, 83.
[18] Zhao, G., Zhang, C., & Zheng, L. (2017). Intrusion Detection Using Deep Belief Network and Probabilistic Neural Network. Proceedings of the IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), 21–24.
[19] Meng, F., Fu, Y., Lou, F., & Chen, Z. (2017). An Effective Network Attack Detection Method Based on Kernel PCA and LSTM-RNN. Proceedings of the International Conference on Computer Systems, Electronics, and Control (ICCSEC), 25–27.
[20] Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017). Applying convolutional neural network for network intrusion detection. Proceedings of the International Conference on Advances in Computing, Communications, and Informatics (ICACCI), 13–16.
[21] Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. IEEE Access, 5, 21954–21961.
[22] Tang, T. A., Mhamdi, L., McLernon, D., Zaidi, S. A. R., & Ghogho, M. (2016). Deep Learning Approach for Network Intrusion Detection in Software-Defined Networking. Proceedings of the 2016 International Conference on Wireless Networks and Mobile Communications,