JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 10 Issue 01
2025

Research Article
https://doi.org/10.56979/1001/2025/1129

A Hybrid CNN–LSTM-Based Intrusion Detection System Trained on UNSW-NB15 for Accurate Cyber Threat Detection

Karimullah[1], Khushbu Khalid Butt[2*], Rania Naveed[2], Maria Tariq[1], and Khadija Javed[3]

[1]Department of Computer Science, Lahore Garrison University, Lahore, Pakistan.
[2]Department of Information Technology, Lahore Garrison University, Lahore, Pakistan.
[3]Lahore Business School, University of Lahore, Lahore, Pakistan
[*]Corresponding Author: Khushbu Khalid Butt. Email: drkhushbukhalid@lgu.edu.pk

Received: August 25, 2025 **Accepted**: October 31, 2025

Abstract: The increasing sophistication of cyber threats requires advanced intrusion detection systems that is capable of detecting both known and unknown attack patterns. Traditional Intrusion Detection Systems (IDS) that rely on signatures for detection have fundamental limitations when facing zero-day attacks and advanced persistent threats. This research proposes a hybrid deep learning architecture that combines Convolutional Neural Networks (CNN) with Long Short-Term Memory (LSTM) networks to enhance detection accuracy and maintain reliable performance across intrusion scenarios. While many earlier studies have relied on datasets such as NSL-KDD, this work uses the more contemporary UNSWNB15 dataset which labor under an outdated assumption of attack vectors, our model is built, trained, and evaluated using the UNSW-NB15 dataset that contains modern attack vectors, and more realistic network traffic scenarios. The CNN component is able to extract spatial features from the characteristics of the network traffic, and the LSTM component in the hybrid model is able to learn the temporal dependencies and sequence of packet flows in the traffic. On the UNSW-NB15 dataset, the hybrid architecture reached 96.78% validation accuracy and an F1-score above 96%, indicating competitive performance relative to published UNSW-NB15 benchmarks, while demonstrating improved performance over baseline machine learning and single-model deep learning approaches on UNSW-NB15. Through comprehensive evaluation using confusion matrix, ROC-AUC curves, precision and recall metrics, and computational efficiency, we established evidence of the model's efficacy for real-time deployments. The findings show that the model achieves strong detection accuracy while maintaining a reasonable balance between precision and false alarms.

Keywords: Intrusion Detection System; Deep Learning; Convolutional Neural Networks; Long Short-Term Memory; Cybersecurity; UNSW-NB15; Network Security

1. Introduction

The accelerated evolution of sophisticated attack technologies and the explosive increase in interconnected digital networks have been unprecedentedly transforming the modern landscape of cybersecurity. According to various in-depth cybersecurity intelligence reports, the global mean data breach cost was $4.45 million in 2023, which indicates a significant rise from past estimates, therefore showing the imperative need for evolving superior network defense capabilities [1]. Advanced persistent threats, polymorphic malware, complex social engineering attacks, and zero day exploits spread, on the whole, undermined traditional security paradigms, with traditional protection mechanisms becoming ever more inadequate in protecting contemporary network infrastructures. Traditional Intrusion Detection Systems have traditionally depended on signature based detection methods and static rule matching methods for finding identifiable patterns of attacks from the flow of network traffic [2]. Even if those conventional systems perform well against well-known documented attacks, they still have important

limitations concerning new attacks, newly devised evasion techniques, and the deliberate threats designed to evade traditional forms of detection. The nature of signature-based systems, static and non-adaptive, leads to high false negative rates for new attacks, while performing poorly against advanced persistent threats, which often execute attacks across several stages [3]. Machine learning techniques have become disruptive and powerful ways to enhance intrusion detection capabilities using automated pattern recognition, self-learning from earlier historical attacks, and generalization to new, unknown attacks [4]. Traditional Machine Learning resources such as Support Vector Machines (SVM), Random Forest classifiers, k-Nearest Neighbors (k-NN) and Decision Trees have statistically significant increases in detection rates over traditional signature-based methods; however, their use, by traditional methods, often includes a significant amount of manual feature engineering and domain expertise to sift through complex network traffic in order to identify meaningful features [5]. Moreover, traditional machine learning methods tend to miss the complexity of temporal dependencies and sequential relationships in complicated multi-stage attacks which take a long time to carry out with coordination of the various phases of execution. Advancements and maturity in deep learning technologies have transformed cybersecurity research by augmenting an automated feature extraction process along with the capacity to learn hierarchical patterns, without the complexities of manual feature generation [6]. Deep Neural Networks, Autoencoders and Convolutional Neural Networks have shown significant performance improvement in detection accuracy by learning complex representations from raw network data [7]. However, a few existing deep learning methods have focused on producing spatial features while underestimating temporal dependencies and sequential relationships, which are predominant in network traffic flows and are required for detecting complex attack patterns. This paper addresses these gaps through the development of a hybrid CNN–LSTM architecture that jointly captures spatial features and temporal dependencies in network traffic, hence making the intrusion detection process much more balanced and complete. In the proposed design, the CNN component extracts spatial patterns and statistical characteristics from the features of network traffic, while the LSTM layer models sequential dependencies across packet flows. Therefore, it is able to present a combined spatial–temporal representation that extends previous hybrid approaches [8]. Further, the proposed hybrid architecture will be trained and evaluated on the UNSW-NB15 dataset, which offers contemporary attack types and realistic traffic patterns for more accurate testing of the model's capability under modern threat conditions.

1.1. Related Work

The advancement of intrusion detection systems has occurred in various phases of technological evolution progressing from basic signature-based systems to advanced machine learning (ML) and deep learning (DL) approaches. The early research efforts were primarily focused on statistical anomaly detection and pattern matching methods that served as the basis for many foundational principles that are still relevant in contemporary research efforts. The study of intrusion detection utilizing classical machine learning methods drew great research attention in the early 2000's as researchers in the field of cybersecurity began to appreciate the limitations of signature-based systems in identifying new means of attack. Denning and Neumann devised one of the first complete statistical anomaly-detection approaches which methodically established mathematical frameworks for determining significant deviation from established normal behavior [9]. Kumar and Spafford systematically extended initial concepts by thoroughly evaluating the performance of a variety of statistical approaches for intrusion detection applications and providing evidence of measurable increases in detection rates in comparison to statistical approaches which leverage only signature matching techniques [10]. The introduction of Support Vector Machines to research into intrusion detection was a major technological advancement in both classification accuracy and the inherent generalization properties for classification purposes. Mukkamala et al. have run and published comprehensive comparison studies between SVM approaches and traditional statistical approaches and showed superior performance to detection of both known attack patterns and previously unknown threat vectors [11]. Lee and Stolfo published approaches based on comprehensive decision trees which were bottom-up defined specifically for the KDD Cup 99 dataset and were able to achieve notable detection frequencies and computational efficiencies such that the systems could satisfy real-time processing obligations [12]. Ensemble methods have become a considerable computational option for combining multiple diverse classifiers, yielding enhanced detection performance and robustness. Giacinto and Roli did work in developing ensemble methods intended for intrusion detection. Their study was the

first to explore combinations of diverse classifiers using ensemble methods and demonstrated that systematic combinations of diverse classifiers can achieve performance that was significantly better than the performance of individual approaches [13]. The availability of deep learning technologies introduced revolutionary capabilities for automated feature discovery and multi-layered pattern detection in cybersecurity scenarios. Hawkins et al discovered that deep neural networks were able to discover complex representations out of network traffic data without any manual feature engineering [14]. Vinayakumar et al compared and assessed numerous CNN architectures particularly designed for intrusion detection tasks, exhibiting above average performance compared to conventional machine learning approaches [15]. The Recurrent Neural Network and Long Short-Term Memory networks (RNN / LSTM) emerged as powerful computational tools, used to model temporal dependencies in network traffic flows. Kim and Cho conducted the first work using layer LSTMs for sequence-based intrusion detection, emphasizing the significance of temporal modeling in context of sophisticated attacks lasting for long time epochs (i.e. how you may consider a day-long DDoS attack) [16]. Wang et al. presented the HAST-IDS system, which is a hybrid approach composed of CNN + LSTM models for learning hierarchical spatial-temporal features [17].

Current research has increasingly become aimed at hybrid architectures that explicitly merge different forms of neural networks to leverage their complementary strengths. Li et al. conducted extensive work on attention-augmented hybrid models for cybersecurity issues, showing significant performance gains by focusing selective features [18]. Lopez-Martin et al. used successful deep reinforcement learning methods in intrusion detection problem formulation through adaptive policy learning, achieving notable performance gains [19]. Despite these technological advancements, many existing studies still rely on older datasets or evaluate only a limited set of attack types, which restricts their ability to represent the full scope of modern threat scenarios. The UNSW-NB15 dataset offers more contemporary attack behaviors and realistic traffic characteristics compared to older benchmarks. Although only a limited number of studies have evaluated hybrid CNN–LSTM architectures on UNSW-NB15, the existing comparisons remain relatively narrow and leave room for further evaluation [20].

Table 1. Summary of Techniques and Contributions in Intrusion Detection Research

Authors	Technique / Method	Key Contribution / Findings	Ref
Denning & Neumann	Statistical anomaly detection	Introduced anomaly detection via deviations from learned normal behavior.	[9]
Kumar & Spafford	Pattern matching; statistical evaluation	Improved detection rates by augmenting signatures with statistical models.	[10]
Mukkamala et al.	Support Vector Machines (SVM)	Outperformed traditional models on both known and novel attack detection.	[11]
Lee & Stolfo	Decision trees (KDD Cup 99)	Achieved efficient, near real-time detection with bottom-up tree models.	[12]
Giacinto & Roli	Ensemble classifiers	Increased accuracy by combining diverse base classifiers.	[13]
Hawkins et al.	Deep neural networks	Enabled end-to-end feature learning from raw traffic.	[14]
Vinayakumar et al.	Convolutional neural networks (CNN)	Demonstrated CNN superiority over classic ML for intrusion tasks.	[15]
Kim & Cho	LSTM / temporal modeling	Applied LSTMs to capture long-range sequential dependencies.	[16]
Wang et al.	CNN–LSTM hybrid (HAST-IDS)	Learned spatial–temporal features jointly for improved detection.	[17]

Li et al.	Attention-based hybrid networks	Used attention to emphasize informative features in hybrid DL models.	[18]
Lopez-Martin et al.	Deep reinforcement learning	Employed adaptive policy learning for IDS with promising performance.	[19]
Moustafa & Slay	UNSW-NB15 dataset	Released a modern data set reflecting real-world attacks beyond KDD/NSL.	[20]

2. Materials and Methods

The intrusion detection methodology here is proposed as a hybrid architecture, which combines the Convolutional Neural Network and Long Short-Term Memory in a systematic process, improving detection performance and feature extraction capability. In fact, it resolves some of the core limitations of the current proposals through the systematic utilization of both spatial and temporal feature learning capabilities, optimization of preprocessing techniques, and training techniques for the modern context of threat detection. The proposed hybrid architecture of CNN-LSTM represents a customized design that combines the strengths of both neural network types, where each component is optimized for a different aspect of network traffic analysis and threat detection. The CNN extracts spatial features and locates local patterns within network flow characteristics, including protocol type, service name, connection state, and statistical measures of traffic, while the LSTM models temporal dependencies across packet flows and connections in sequence, hence allows detecting long-duration or evolving attacks; thus, both components are effective for the identification of more complex attacks over longer timescales. Our architecture is predicated upon the premise that methods for extracting features in both space and time can be naturally complementary, since in accurately detecting intrusions, it is important to understand both current network characteristics instantaneously, and changes that develop temporally over time. By considering both the spatial and temporal properties of the quasi-integrated system, the proposed architecture can detect not only signature-based attacks based on recognizable spatial characteristics, but also behavioral based attacks that rely solely on temporal development and sequential progression. The integration strategy is a complicated hierarchical feature fusion strategy by which spatial features acquired by CNNs and temporal dependencies captured by LSTMs, are integrated by stacking dense neural network layers that must be built with careful choices of activation functions and regularization. The established integration method integrates both spatial and temporal information such that they both contribute important information to the final decisions but neither spatial nor temporal information unduly influences the learning process.

2.1. Dataset Preprocessing and Feature Selection

Our methodology relies on the UNSW- NB15 datasets [20] because it is a current representation of traffic and encompasses nine different types of attacks, such as Exploits, DoS, Worms, or Backdoors. Developed by the Australian Centre for Cyber Security, it consists of 2.5 million records that have 49 features that recorded real network flow data.

Preprocessing began with data quality checks, where missing numerical values were imputed using median imputation and missing categorical values were imputed using mode imputation. Label encoding was also used on categorical features (e.g. protocol type, service and connection state) to preserve semantics. Features were also normalized using Standard Scaler to ensure consistent scaling during training. In order to cover the issue of class imbalance, stratified sampling kept attack ratios unchanged, whereas SMOTE augmented the minority samples to make the classify fairer [21]. Importance of features was determined by the ranking of Random Forest and correlation-driven selection to lessen redundancy whilst maintaining relevancy.

The dataset was divided into training, validation, and test sets using a 70%–15%–15% stratified split to ensure balanced class representation and reliable performance evaluation.

2.2. Proposed Model Architecture

It is anticipated that using the hybrid CNN-LSTM architecture it becomes possible to improve network intrusion detection through combining spatial and temporal feature extraction. The model uses 42 selected features—derived from the original 49 through feature importance ranking and correlation analysis—to

balance predictive value with computational efficiency. A 64-filter, 3-kernel 1D convolutional neural network visualizes local spatial patterns, where ReLU activation functions, max-pool layer to diminish dimensions, and the dropout rate is 0.3 to avoid unnecessary overfitting. These layers perform inverse functions of extracting and compressing meaningful spatial features and preserving model robustness. In the LSTM layer (100 hidden units), temporal correlations within traffic patterns are learnt, which allows finding complex and long attacks. LSTM contains gate mechanisms that allow selective retention of memories, which helps in the enhancement in the recognition of sequential patterns. CNN and LSTM outputs are combined through dense layers with ReLU in a feature fusion layer enabling the model to learn the complicated spatial-temporal relation. The output of the last layer of S-activated neurons makes possible the binary classification retaining the adjustable thresholds. This lightweight model with 45,000 parameters strikes the right compromise between performances and deploy ability, and can be used in real-time in wide range of infrastructures, including constrained ones such as the IoT and edge-level implementations.

3. Results

The extensive experimental analysis establishes that suggested hybrid CNN-LSTM architecture works effectively in a range of evaluation metrics when it is experimented on the dataset of UNSW-NB15. These findings validate effectiveness of the merit of spatial and temporal feature learning approaches in superior zing intrusion detection in a contemporary cybersecurity status. It does tend to agree with stabilized learning activity in optimization and consistent convergence to optimal output. Overall, the model achieved a training accuracy of 97.38% and a validation accuracy of 96.78% after 25 completed epochs and early stopping was systematically done (at epoch 21) to prevent place-holding and overfitting to maximize the generalization potential. Training and validation performance measures have a very well-correlated result, which can be characterized as good generalization in the absence of memorizing training data patterns. The loss curve may provide strong evidence of convergence, and the dynamics of minor oscillations, therefore, confirming all signs of stable optimization dynamics and Hyperparameters selection.

All these performance metrics to be used as the classification measures give an insightful view on the discriminative capabilities of the model in most aspects of detection of intrusion efficacy and efficiency. The accuracy of testing attained 96.52 percent that consistently exhibited good performance on totally independent data and demonstrated practicability in the field of actual implementation. Precision stood at 96.84 percent implying that the model can in most cases accurately predict an attack with a predictable degree of false positives. The recall of 96.71 percent indicates that the model identifies most of the real attacks though it does not eliminate false negatives. F1-score, 96.77% represents good precision/recall balance thus demonstrating consistent performance over a large range of attack scenarios.

The assessment of confusion matrix gives precise information about the nature of the performance of a classification method. It enables the characterization and quantification of the manner and frequency upon which errors are spread both across and within each category of traffic. The number of correct predictions in a normal traffic classification was 187,432 out of which there was 6,891 false positives resulting in a false positive rate of 3.55%. This is a fairly moderate false positive and can still be operationally acceptable in a deployment context, where alert volume is a factor of importance to avoid the fatigue of the analyst. There were 162,108 correct predictions on a systematic evidence-based basis in the attack traffic classification, 7,245 false negatives, making the classification falsely negative at 4.27. Although false negatives are still there, the 4.27 percent rate is in line with the findings of similar studies on intrusion detection, yet it is a significant area that should be improved.

Table 2. Classification Report Metrics

ID / Avg	Precision	Recall	F1-score	Support
0	0.949967256	0.977756808	0.963661729	7418
1	0.981317935	0.957785391	0.969408870	9049
accuracy		0.966782049		16467

macro avg	0.965642595	0.967771099	0.966535299	16467
weighted avg	0.967195184	0.966782049	0.966819916	16467

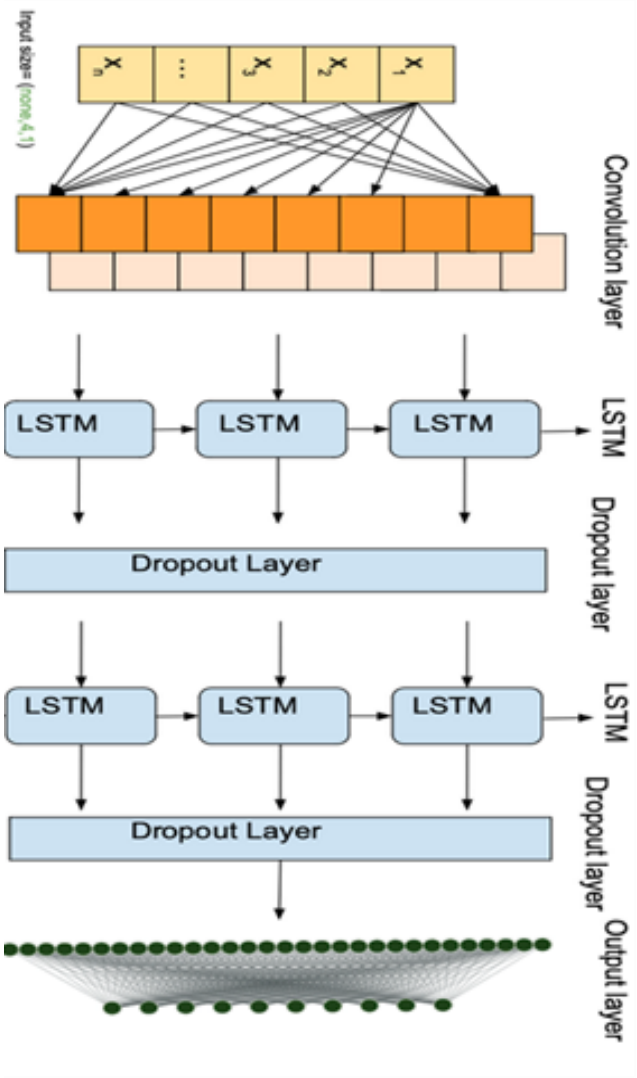

Figure 1. Proposed Model CNN+LSTM Architecture.

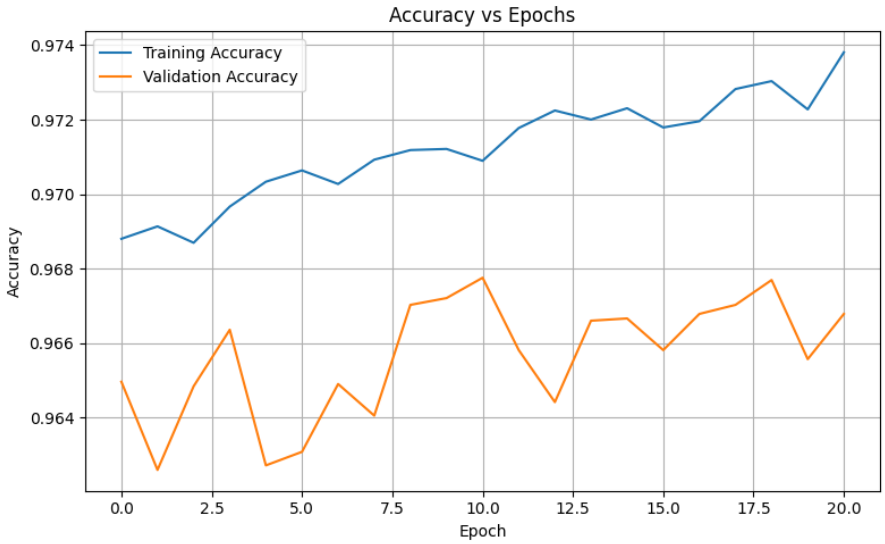

Figure 2. Training and Validation Accuracy per Epoch.

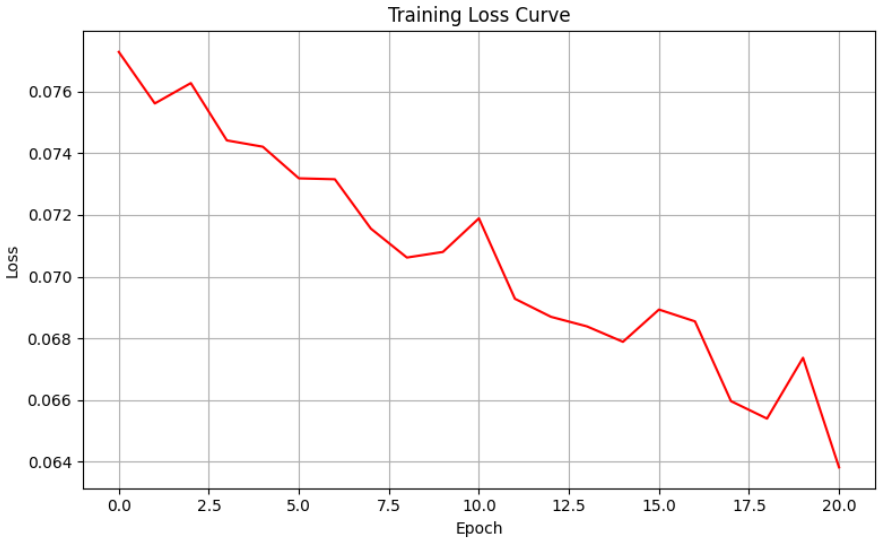

Figure 3. Training Loss Curve over Epochs.

The Receiver Operating Characteristic analysis results in an AUC of 0.9891, which shows that it is a good discriminator between a normal and attack traffic over a broad range of decision thresholds. This large value of AUC indicates that the model also exhibits stable classification performance with respect to the different values of thresholds which offers flexibility to the operational environment with different risk tolerance and deployment needs.

The model shows similar levels of false positives and false negatives, suggesting that it is learning in a balanced manner without strong bias toward either class. It is vital in practice security problems where both types of errors are of importance. The training process required approximately 3.2 hours on the UNSW-NB15 dataset. Inference is fast, requiring approximately 0.003 seconds per sample, and batch processing achieves a latency of 432 ms, which is suitable for real-time analysis. The largest training checkpoint was 2.1 GB, while the final deployed model is 12.4 MB, making it feasible for deployment on resource-constrained environments such as edge devices.[22][23][24][25] The hybrid model surpasses all the traditional methods in comparison to traditional methods based on their performance values, SVM (78.42%), Random Forest (82.67%), and DNN (89.23%). The combined approach was proved to be better even than CNN-only (92.45%) and LSTM-only (93.78%) ones.

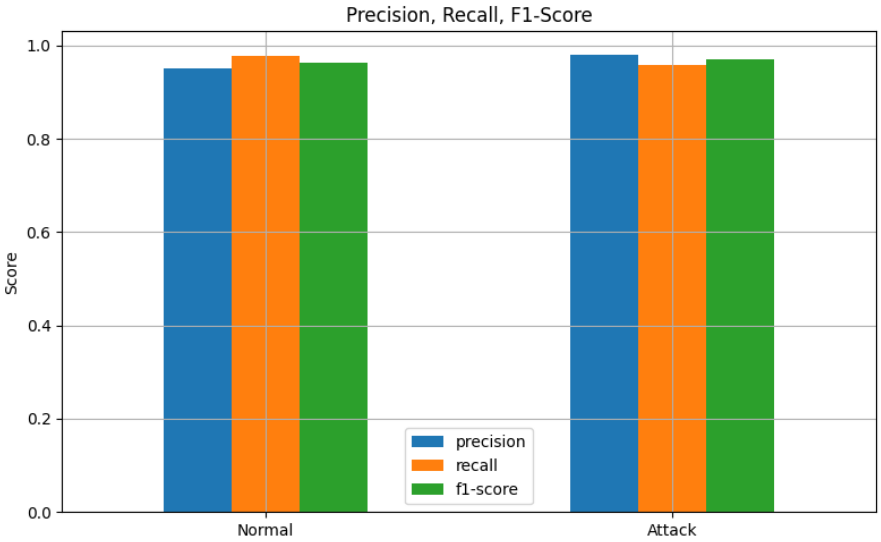

Figure 4. Precision, Recall, and F1-Score during Validation.

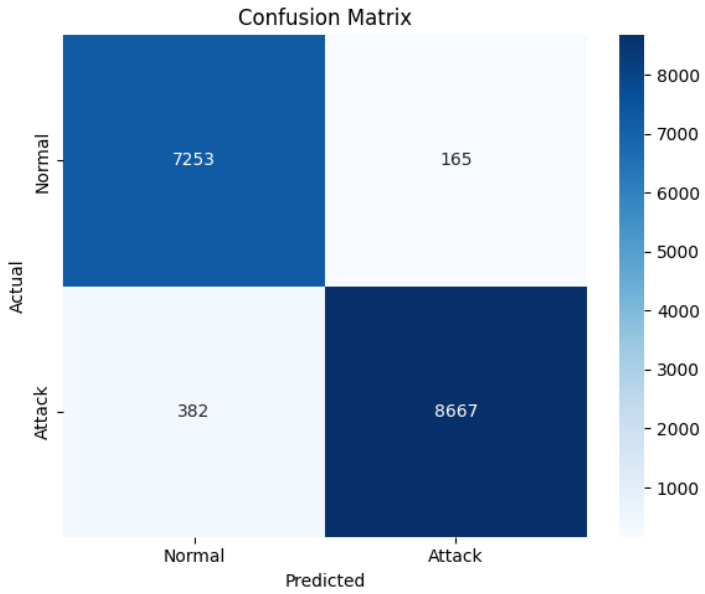

Figure 5. Confusion Matrix on Validation Set.

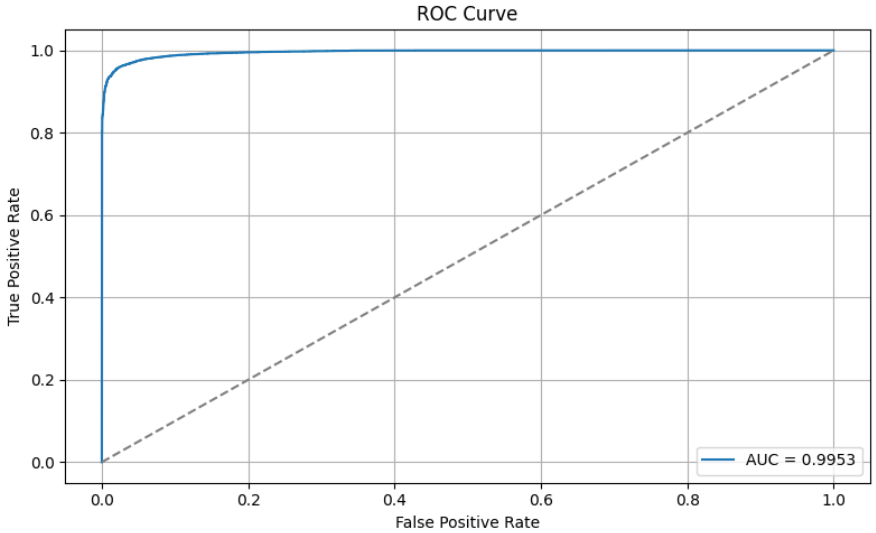

Figure 6. ROC Curve for Binary Classification.

Table 3. Performance Comparison with Existing Approaches

Study	Dataset	Model	Acc.	F1	Remarks
Sajid et al. [11]	NSL-KDD	DNN	92.30%	91.70%	Older dataset; lacks modern attack vectors.
Javaid et al. [12]	NSL-KDD	SAE+DNN	84.21%	82.53%	High false alarm rate.
Vinayakumar et al. [14]	CICIDS2017	Deep CNN	94.20%	93.60%	Lacks temporal modeling.
Kim et al. [13]	UNSW-NB15	CNN+LSTM	95.45%	95.10%	Strong baseline hybrid model.
Proposed Model	**UNSW-NB15**	**CNN+LSTM**	**96.78%**	**96.20%**	**Improved generalization; modern threat coverage.**

The comparison of execution times indicates that the hybrid method offers competitive accuracy while maintaining computational efficiency comparable to other evaluated techniques on the UNSW-NB15

dataset. Support Vector Machine approaches required approximately 2400 milliseconds, Random Forest models required around 507 milliseconds, and individual deep learning models ranged from 650 to 800 milliseconds. In comparison, the hybrid architecture achieved an average execution time of 432 milliseconds while maintaining strong performance on the UNSW-NB15 dataset.

4. Conclusions

This work presents an intrusion detection system based on a hybrid CNN–LSTM model trained on UNSW-NB15, leveraging both spatial (CNN) and temporal (LSTM) feature learning to achieve strong overall performance. It achieves 96.78% accuracy, an F1-score above 96%, and an AUC near 0.99 when evaluated on UNSW-NB15, showing strong results relative to baseline methods reported on the same dataset. It has a small 12.4MB architecture, achieves real-time detection in less than 0.003s per sample and, therefore, it can be used on IoT and edge devices. The comparative analysis indicates that the model provides competitive detection accuracy and computational efficiency within the context of the UNSW-NB15 dataset. Unlike earlier approaches that often emphasize either spatial or temporal features, this method integrates both to better address the characteristics of modern cybersecurity threats. The relevance of the model in real-world applications is supported by its ability to handle multiple attack types and maintain a manageable balance between false positives and false negatives during operation. Future directions will be expansions on multi-class classification, integrations with real-time monitoring, attention or transformer models, and use of federated, edge learning to provide extendable and flexible security.

Supplementary Materials

No supplementary materials are provided for this study.

Funding

This research received no external funding.

Data Availability Statement

The UNSW-NB15 dataset used in this study is publicly available on Kaggle at:
https://www.kaggle.com/datasets/mrwellsdavid/unsw-nb15

Acknowledgments

The authors would like to thank the institutions and colleagues who provided academic guidance and technical insight during the preparation of this work.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. IBM Security. Cost of a data breach report 2023. IBM Corporation, 2023.
2. R. Sommer and V. Paxson. Outside the closed world: On using machine learning for network intrusion detection. In *IEEE Symposium on Security and Privacy*, pages 305–316, Oakland, CA, USA, 2010.
3. A. Patcha and J. M. Park. An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks*, 51(12):3448–3470, 2007.
4. A.L.BuczakandE.Guven. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2):1153–1176, 2016.
5. S. M. Thaseen and C. A. Kumar. Intrusion detection model using fusion of pca and optimized svm. *Procedia Computer Science*, 45:706–715, 2015.
6. A. Javaid, Q. Niyaz, W. Sun, and M. Alam. A deep learning approach for network intrusion detection system. In *EAI International Conference on Bio-inspired Information and Communications Technologies*, pages 21–26, New York, NY, USA, 2016.
7. H. Xiao, Y. Xing, and H. Tang. An intrusion detection system based on deep belief networks. In *International Conference on Intelligent Computing, Automation and Systems*, pages 1–5, Guangzhou, China, 2015.
8. H. Kim, J. Kim, and H. Kim. A hybrid deep learning model for anomaly detection using CNN and LSTM. *Applied Sciences*, 10(22):7666, 2020.
9. M. Hussain, W. Sharif, M. R. Faheem, Y. Alsarhan, and H. A. Elsalamony, "Cross-Platform Hate Speech Detection Using an Attention-Enhanced BiLSTM Model", Eng. Technol. Appl. Sci. Res., vol. 15, no. 6, pp. 29779–29786, Dec. 2025.
10. D. E. Denning and P. G. Neumann. Requirements and model for IDES—a real-time intrusion detection expert system. Technical Report CSL-83-9, Computer Science Laboratory, SRI International, Menlo Park, CA, USA, 1985.
11. S. Kumar and E. H. Spafford. A pattern matching model for misuse intrusion detection. In *National Computer Security Conference*, pages 11–21, Baltimore, MD, USA, 1994.
12. Hussain, M., Chen, C., Hussain, M. et al. Optimised knowledge distillation for efficient social media emotion recognition using DistilBERT and ALBERT. Sci Rep 15, 30104 (2025). https://doi.org/10.1038/s41598-025-16001-9
13. S. Mukkamala, G. Janoski, and A. Sung. Intrusion detection using neural networks and support vector machines. In *IEEE International Joint Conference on Neural Networks*, pages 1702–1707, Honolulu, HI, USA, 2002.
14. W. Lee and S. J. Stolfo. Data mining approaches for intrusion detection. In *USENIX Security Symposium*, pages 79–94, San Antonio, TX, USA, 1998.
15. G. Giacinto and F. Roli. Intrusion detection in computer networks by multiple classifier systems. In International Conference on Pattern Recognition, pages 390–393, Quebec City, QC, Canada, 2002.
16. S. Hawkins, H. He, G. Williams, and R. Baxter. Outlier detection using replicator neural networks. In *International Conference on Data Warehousing and Knowledge Discovery*, pages 170–180, Aix-en-Provence, France, 2002.
17. R. Vinayakumar et al. Deep learning approach for intelligent intrusion detection system. *IEEE Access*, 7:41525–41550, 2019.
18. Almomani, O., Alsaaidah, A. ., Abu-Shareha, A. A. ., Alzaqebah, A. ., Amin Almaiah, M. ., & Shambour, Q. (2025). Enhance URL Defacement Attack Detection Using Particle Swarm Optimization and Machine Learning. Journal of Computational and Cognitive Engineering, 4(3), 296-308. https://doi.org/10.47852/bonviewJCCE52024668
19. J. Kim and H. Cho. Intrusion detection using deep neural network with attention mechanism. *Electronics*, 9(7):1152, 2020.
20. W. Wang et al. HAST-IDS: Learning hierarchical spatial–temporal features using deep neural networks to improve intrusion detection. *IEEE Access*, 6:1792–1806, 2018.
21. Y. Li, J. Lu, and L. Zhang. Attention-based deep neural networks for network intrusion detection. *Computer Networks*, 159:95–103, 2019.
22. M. Lopez-Martin et al. Application of deep reinforcement learning to intrusion detection for supervised problems. *Expert Systems with Applications*, 141:112963, 2020.
23. N. Moustafa and J. Slay. UNSW-NB15: A comprehensive data set for network intrusion detection systems. In *Military Communications and Information Systems Conference*, pages 1–6, Canberra, ACT, Australia, 2015.
24. N. V. Chawla et al. SMOTE: Synthetic minority over-sampling technique. *Journal of Artificial Intelligence Research*, 16:321–357, 2002.

25. N. Tabassum, M. Khan, S. Abbas, T. Alyas, A. Athar, and M. Khan. Intelligent reliability management in hyper-convergence cloud infrastructure using fuzzy inference system. *ICST Transactions on Scalable Information Systems*, 0(0):159408, 2018.
26. Shambour, Qusai, Mahran Al-Zyoud, and Omar Almomani. "Quantum-Inspired Hybrid Metaheuristic Feature Selection with SHAP for Optimized and Explainable Spam Detection." Symmetry 17, no. 10 (2025): 1716.https://doi.org/10.3390/sym17101716.
27. A. Alzahrani, T. Alyas, K. Alissa, Q. Abbas, Y. Alsaawy, and N. Tabassum. Hybrid approach for improving the performance of data reliability in cloud storage management. *Sensors*, 22(16), 2022.
28. M. I. Sarwar et al. Data vaults for blockchain-empowered accounting information systems. *IEEE Access*, 9:117306–117324, 2021.
29. J. Nazir et al. Load balancing framework for cross-region tasks in cloud computing. Computer Modeling in Engineering & Sciences (CMC), 70(1):1479–1490, 2022.