Sarcouncil Journal of Engineering and Computer Sciences

ISSN(Online): 2945-3585

Volume- 02| Issue- 11| 2023

Research Article **Received:** 20-10-2023| **Accepted:** 15-11-2023 | **Published:** 30-11-2023

CNN-LSTM Hybrid Architecture for Accurate Network Intrusion Detection for Cybersecurity

Dinesh Rajendran,[1] Vaibhav Maniar,[2] Vetrivelan Tamilmani,[3] Venkata Deepak Namburi,[4] Aniruddha Arjun Singh Singh,[5] and Rami Reddy Kothamaram,[6]

[1]*Coimbatore Institute of Technology, MSC. Software Engineering*
[2]*Oklahoma City University, MBA / Product Management,*
[3]*Principal Service Architect, SAP America*
[4]*University of Central Missouri, Department of Computer Science,*
[5]*ADP, Sr. Implementation Project Manager*
[6]*California University of management and science, MS in Computer Information systems,*

Abstract: Cyber threat network security is of importance because the technology is progressively turning out to be important in the era of heightened digitalization. Improving cyber intrusion detection systems is crucial because cyberattacks on critical infrastructure are becoming more targeted and sophisticated. Using the NSL-KDD dataset for IDS is best accomplished with a CNN-LSTM model, according to the research. The workflow contains expensive preprocessing such as label encoding, feature selection, and z-score normalization, and 70 30 train-test splits. The spatial features of the traffic data are learnt with CNN and the sequential dependencies are performed by LSTM, which allows the robust classification of normal and attack traffic. The suggested model outperforms standard classifiers like SVM and LR experimentally, with results of 94.32% accuracy, 99.32% precision, 97.88% recall, and 98.60% F1-score. Based on these findings, CNN-LSTM hybrid is an intriguing method for enhancing detection accuracy while decreasing false positives. Deep learning-based intruder detection systems could help improve cybersecurity, but further research is needed to evaluate their performance on new data, address class imbalance, and enable real-time operation, as the study suggests.

Keywords: Cybersecurity, Attack Detection, Network Security, Classification, Machine Learning, Attack Detection, Intrusion Detection System (IDS), Hybrid Deep Learning.

INTRODUCTION

A "network attack" is any concerted attempt by malicious actors to steal data or disrupt services from a computer network. The worldwide economy suffers as a result of these attacks, as they jeopardize data's secrecy, integrity, and availability, and, in most cases, have far-reaching financial consequences (Abubakar, A. I. *et al.*, 2015). With the growing access to wireless technologies, cybercriminals can access systems remotely, rather than physically, by exploiting weaknesses located at a distance, making existing networks more susceptible to attacks and malicious use.

Multi-layered protection, including firewalls, encryption, access control, and authentication systems, is also used to safeguard against such threats through cybersecurity systems (Sarker, I. H. *et al.*, 2020). Nevertheless, these traditional solutions are often insufficient for monitoring complex or unfamiliar forms of attacks (Liu, G., & Zhang, J. 2020). IDSs are an integral part of contemporary cybersecurity architectures. The second layer of protection that constantly monitors network traffic and system activity is IDSs, which can identify various types of harmful behavior, such as a DoS attack, unauthorized access, or data tampering (Ferrag, M. A. *et al.*, 2020; Kushwaha, A. *et al.*, 2016). Following the benign traffic patterns and recognizing them in relation to abnormal conduct, IDSs are essential in enhancing the system's security.

The recent advances of the artificial intelligence (AI) have brought the potent strategies to the creation of the intelligent IDSs. It has been established that machine learning (ML) system is effective at identifying known and making predictions about new threats, particularly when there is adequate training data (Liu, H., & Lang, B. 2019; Maddali, G. 2025; Thapliyal, A. *et al.*, 2009). The ML-based IDSs can dynamically learn as data streams unlike the traditional approach that needs significant familiarity of the field. Moreover, a more beneficial method of working with large and complex data is one of the sub-branches of ML, deep learning (DL), as it allows extracting high-level features automatically and providing an impetus to the accuracy of detection (Neeli, S. S. S. 2019).

The ability of hybrid networks to integrate CNNs with LSTMs in intrusion detection has been more encouraging than that of other deep learning models (Buczak, A. L., & Guven, E. 2015; H. P.

***Corresponding Author:** Dinesh Rajendran

DOI- https://doi.org/10.5281/zenodo.17516985

Kapadia, 2020). CNNs are famous for extracting the local spatial characteristics of network traffic, but LSTMs have the capability of extracting the time series dependence of sequential data (Neeli, S. S. S. 2019). A CNN-LSTM hybrid model can achieve high accuracy in detecting network intrusions and classification through spatial and temporal learning.

Motivation and Contributions of the Study

A major threat to network security is the growing sophistication of cyberattacks. The limited ability of traditional intrusion detection algorithms (such as LR and SVM) to recognize patterns of attacks in network data based on location and time leads to poor detection rates and a high rate of FP. The contemporary networked environment demands a superior framework in the sense of the capability to acquire high-level characteristic representations and sequential constraints with the likelihood of adequately categorizing a range of types of attacks. The need to construct a reliable IDS that may help fill these gaps and strengthen cybersecurity prompted this study. Among the things that this study offers are:

- The NSL-KDD dataset, which included U2R attacks, Probe, R2L, and DoS was used to assess all parts of intrusion detection.
- Performed a lot of pre-processing (label encoding, feature selection and normalization) to improve model efficiency.
- Introduced a CNN-LSTM hybrid network, a combination of the two methods of obtaining spatial features on network data and temporal correlations.
- Produced a robust, scalable and stable intrusion detection architecture capable of recognizing different kinds of attacks with minimum false alarms.
- To look at all of the models and find out how reliable and useful hacking recognition is, use key measures like recall, F1score, accuracy, and ROC-AUC.

Justification and Novelty

Cyber threats are getting more complicated, and old ways of finding intrusions don't always work because they don't take into account how modern network data moves and changes over time. And that is precisely why they need to conduct this research. This research recommends an LSTM-CNN hybrid, which combines the best features of the two networks, to address these problems. This setup integrates CNN's strong feature extraction skills with LSTM's stringent sequence learning capabilities. This groundbreaking study develops the first-ever method to improve intrusion detection using a convolutional neural network (CNN) and a long short-term memory (LSTM) model that learns about both spatial and temporal information. On the NSL-KDD dataset, the model outperforms the traditional techniques in terms of precision, F1-score, accuracy, and recall. The proposed paradigm offers a novel approach to developing an efficient IDS that enhances cybersecurity by integrating pre-processing with rigorous evaluation.

Organization of the Paper

The paper is structured in the following way: Section II Covered Cybersecurity IDS Research. Section III delves into the dataset and technique. Section IV delves into the discussion of the experimental results. The author summarises his key points and suggests future study directions in Section V, the final section of the work.

LITERATURE REVIEW

In this section, the Network IDS in Cybersecurity is fully reviewed.

Karanam, Pattanaik and Aldmour (2020) present a fresh method for detecting intrusions using CNNs and LSTMs. This research tackles the problem of unbalanced data sets by extracting features from input data using CNNs. Then, the features are passed on to the LSTM for sequence analysis. Considering the overall number of instances, the weight of each class's training examples is calculated using the cost function technique. Another way to reduce processing cost is by importing raw input data in matrix (image) format. Test the LSTM-CNN model on the classic NSL-KDD dataset to see how well it performs. Impressively, the model achieves a detection rate of 96.75% and a training accuracy of 99.6% in the data (Karanam, L. *et al.,* 2020).

Bachar, Makhfi and Bannay (2020) offer a fresh method for detection intrusions in networks with the use of ML. A behavioural IDS is relied upon by the method to detect novel assaults, as opposed to a signature database. To run the support vector machine for classification, utilize two cores: one for Gaussian and one for polynomial. The UNSW-NB15 is used for the model's testing and training phases. In contrast to the other classification models (ANN, Rf, MLP), the DR results are intriguing (Bachar, A. *et al.,* 2020).

Latif, *et al.,* (2020) IDS monitors network traffic continuously to detect various forms of assaults. This technical article presents an IIoT IDS that

Publisher: SARC Publisher

uses DRaNN. Test the planned method using UNSW-NB15, the most recent IIoT security dataset. The proposed model achieved a remarkable 99.54% accuracy rate, a low FP rate, and corresponding experimental results of top-tier DL IDS approaches. It was also able to identify nine separate attack types. It was demonstrated that the system could perform as expected. Using the suggested method, they achieved a detection rate improvement of 99.51% (Latif, S. *et al.*, 2020).

Khan, *et al*., (2019) DL is a more sophisticated technology and can automatically retrieve sample attributes. This study introduces a CNN-based network IDS tool to solve the limits of existing ML algorithms in this area. The useful characteristics may be extracted mechanically by the model to provide precise intrusion sample classification. Applying the suggested strategy to KDD99 data results in significantly improved intrusion detection accuracy (Khan, R. U. *et al.*, 2019).

Zhiqiang, *et al.,* (2019) demonstrated that DL is the best approach in the given case. DL can also do great classification even when the subjects have complex features and high dimensionality. A DL IDS using the cutting-edge UNSW-NB15 dataset is presented in this paper. Using the correct activation function and attributes should theoretically result in a high accurateness and low false alarm rate when testing on unknown data, according to the experiment's results. Investigators in the area of network IDS have a promising new avenue to explore thanks to evaluation results showing that the suggested classifier beats the competing machine learning models (Zhiqiang, L. *et al.,* 2019).

Srivastava, Agarwal, and Kaur (2019) note that intrusion detection is a rapidly expanding field. In the past, supervised learning methods were employed to identify breaches in the data collected from network traffic. However, not only has traffic volume grown exponentially, but the character of network attacks is evolving as well. Need better detection methods to catch these new forms of attacks. When it comes to finding outliers in network data, ML methods have been extensively studied by researchers. Additional datasets are now available in the public repositories. In this study, innovative ML methods centered on feature reduction were employed to detect anomalies in the newly released dataset. Accuracy rate is now at 86.15% (Srivastava, A. *et al.,* 2019).

Qureshi et al. (2018) A smart intrusion monitoring system can stop bad things from happening before they affect the main network. This research presents a new approach that uses an RNN-IDS. Train NN with variable input and hidden layer densities and learning rates using the industry-standard NSL-KDD dataset for binary classification. Then, analyse the results. Compared the results to those of other systems and measured its performance by looking for new assaults with a detection rate of 94.50% to make sure the strategy was feasible (Larijani, H. *et al.,* 2018). Background research summary comparison is provided in Table I based on data, results, and limitations.

Table 1: Summary of the Related Work on Intrusion Detection for Cybersecurity

Author	**Methods**	**Dataset**	**Key Findings**	**Limitations/Future Work**
Karanam, Pattanaik & Aldmour (2020)	Hybrid CNN-LSTM with cost-sensitive learning for imbalance handling	NSL-KDD	Reliability of 96.75%, and Precision of 99.6%	Needs validation on modern datasets (e.g., UNSW-NB15, CICIDS2017) and real-time environments
Bachar, Makhfi & Bannay (2020)	SVM with Polynomial and Gaussian kernels	UNSW-NB15	Effective behavioral IDS, competitive DR compared to ANN, RepTree, RF, MLP	May face scalability issues with large-scale traffic; future work to test deep learning models
Latif et al. (2020)	DRaNN	UNSW-NB15	Accuracy 99.54%, Detection Rate 99.41%, low false positives	Needs deployment in real-time IIoT environments to test robustness
Khan et al. (2019)	CNN	KDD99	Improved accuracy in intrusion detection through automatic feature extraction	KDD99 is outdated; needs evaluation on modern datasets

Publisher: SARC Publisher

Zhiqiang et al. (2019)	Deep Learning IDS with feature and activation function optimization	UNSW-NB15	High accuracy, reduced false alarm rate, outperformed ML models	Limited to single dataset; needs generalization across multiple datasets
Srivastava, Agarwal & Kaur (2019)	Feature reduction with ML algorithms	New public dataset (not explicitly named)	Achieved 86.15% accuracy in anomaly detection	Accuracy relatively low; scope for applying deep learning for better performance
Qureshi et al. (2018)	Random Neural Network (RNN-IDS)	NSL-KDD	Accuracy 94.50%, effective in detecting novel attacks	Needs testing on more recent datasets; scalability in high-speed networks not addressed

METHODOLOGY

The developed technique for researching intrusion detection systems is structured into numerous steps. Optimizing the model's performance requires pre-processing the data with the NSL-KDD dataset. Next, assign numerical values to the categorical variables using label encoding. Lastly, employ feature selection to reduce dimensionality. Standardizing feature scales is done through data normalization using z-scores. One half for testing and the other half for training. A LSTM- CNN mixture model is subsequently employed in the classification process. When evaluating the model's capacity to identify intrusions in a network, common metrics contain Precision , Recall, F1 Score and Accuracy. Figure 1 shows the entire process.

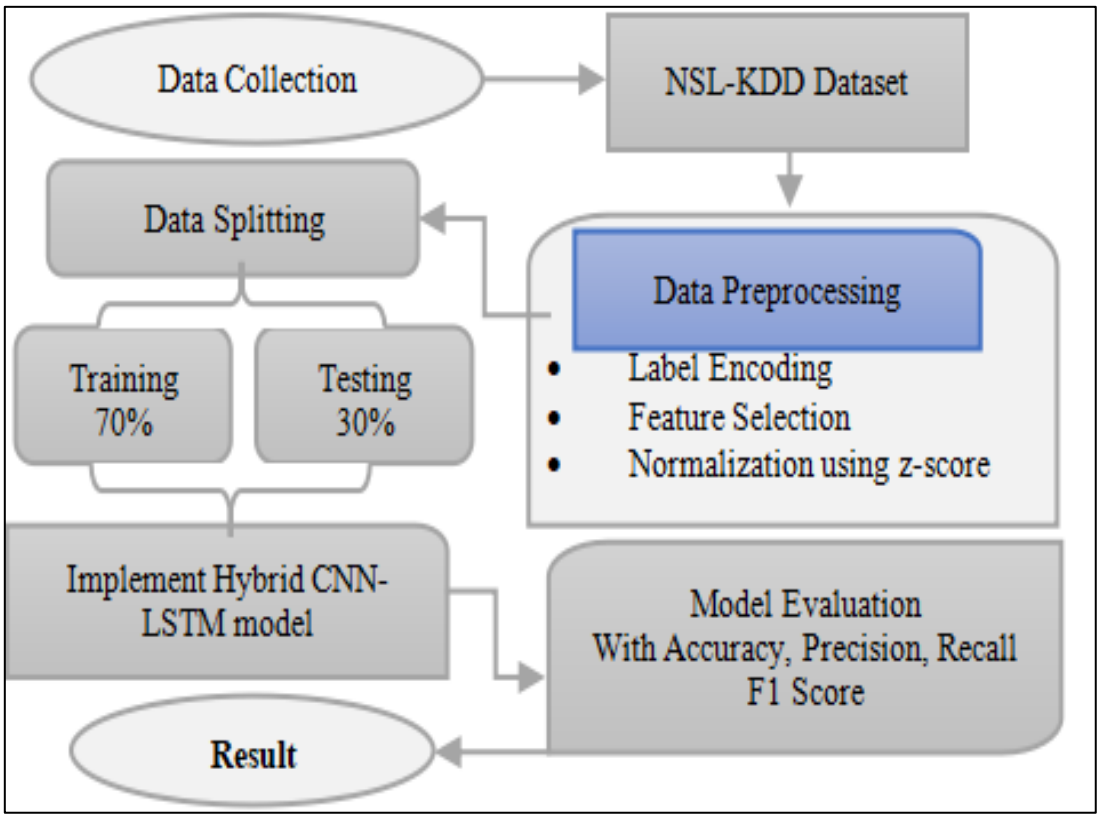

Fig 1: Flowchart for Intrusion Detection in cybersecurity

Brief explanations of each stage of the suggested methodology flowchart are provided below:

Data Collection

This dataset contains 22 unique attack techniques, including denial-of-service attacks, port scanning, R2L, and U2R (illegal access to root super user privileges). Revising and improving the NSL-KDD dataset since KDD'99. In instructions to generate the NSL-KDD dataset on Kaggle, duplicate instances were removed from the KDD'99 dataset. This was done to prevent biased classification results. Here is the visualization graph:

Publisher: SARC Publisher

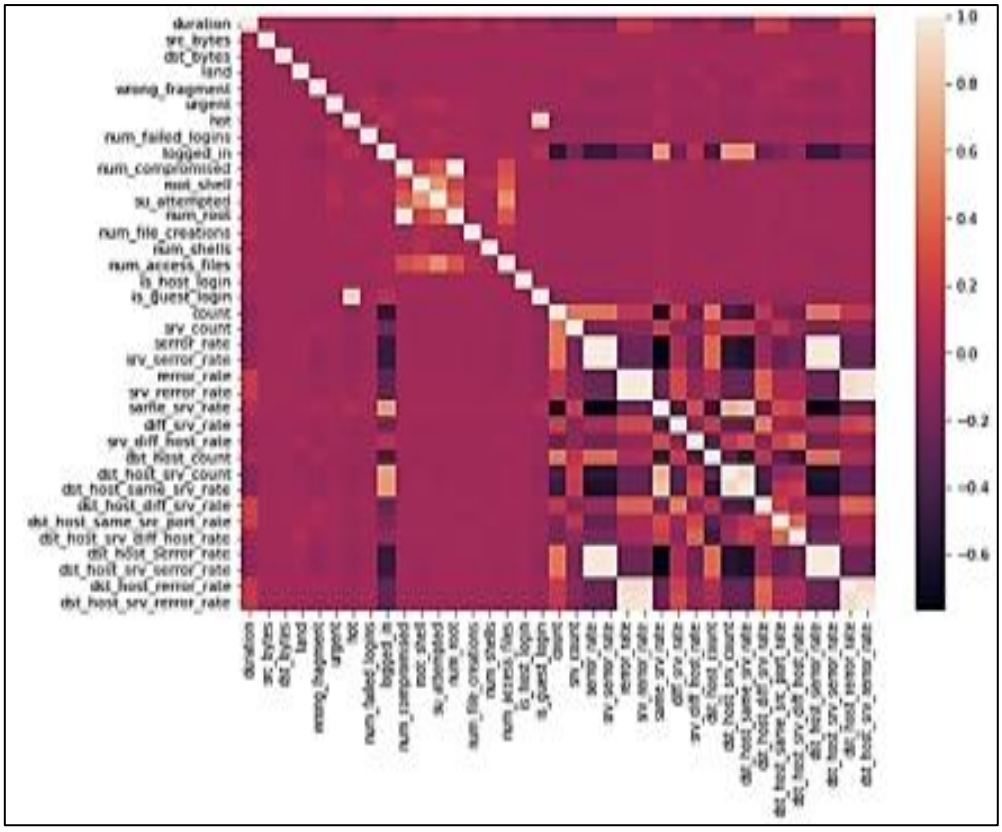

Fig 2: Correlation Heatmap of Dataset Features

The correlation matrix of various dataset attributes is shown in the heatmap Figure 2 up there; the strength of the colours reflects the degree of correlation between pairs of variables. Darker shades, and greater positive or negative correlations by lighter shades represent weak correlations. The diagonal line with white squares represents self-correlation (value = 1). In particular, feature selection and dimensionality reduction in machine learning tasks benefit from this visualization's ability to reveal redundancy in the dataset, highly dependent feature clusters, and multicollinearity among features.

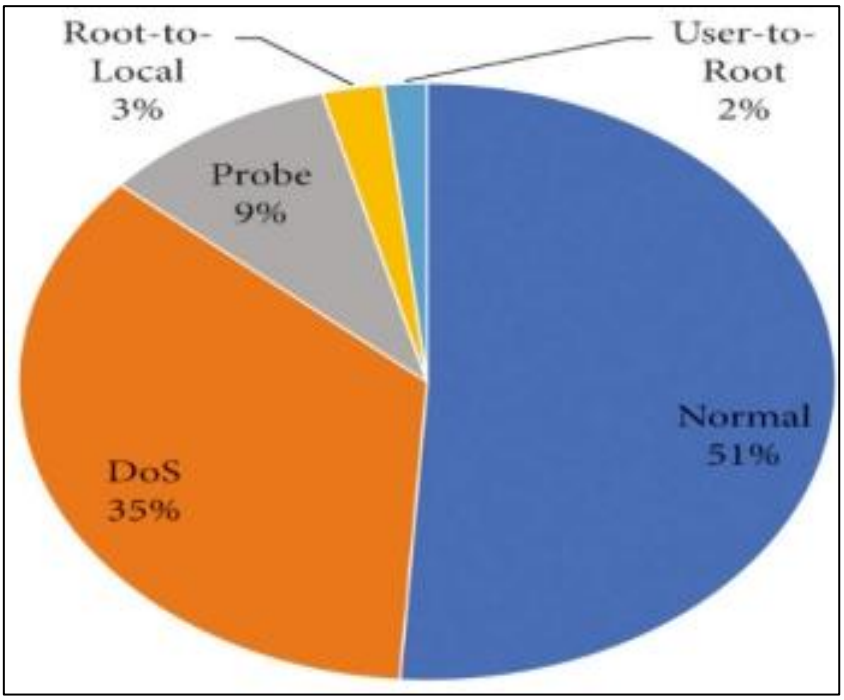

Fig 3: Distribution of Normal and Attack Classes in the Dataset

Publisher: SARC Publisher

Figure 3 displays the dataset's delivery of classes, including the percentage of regular traffic and different sorts of attacks, in a pie chart format. Among the data points, 51% are associated with normal traffic, while 35% are attributed to DoS attacks. Perpetrating attacks account for 9% of assaults, whereas Root-to-Local attacks account for 2% and probing attacks for 3%. Due to this difference, normal and DoS traffic are more salient than other types of traffic; this may impact classification model behavior and require balanced learning techniques, such as resampling.

Data Preprocessing

The pre-processing methods applied improve the effectiveness of the entire system. Data conversion, normalization, label encoding, and feature selection are common components of pre-processing. This is a significant development for the research team working to enhance the model's primary subsystem's detection rates. Discussed below are each of the pre-processing steps:

Label Encoder: The categorical target label was encoded with labels. Values that happened more often were given larger integers, which showed how important they were in terms of attack probability. This approach ensures proper representation of categorical input features ('Proto,' 'sDSb,' 'State,' 'Label,' 'Attack Type,' 'Attack Tool,' 'Cause') without misguiding the model, while preserving the order of the target label for accurate classification.

Feature Selection

Feature selection aims to improve the forecast performance of ML models by removing the least useful features from datasets. It aids in decreasing computing cost, enhancing model accuracy, decreasing overfitting, and reducing dimensionality by removing redundant or irrelevant data.

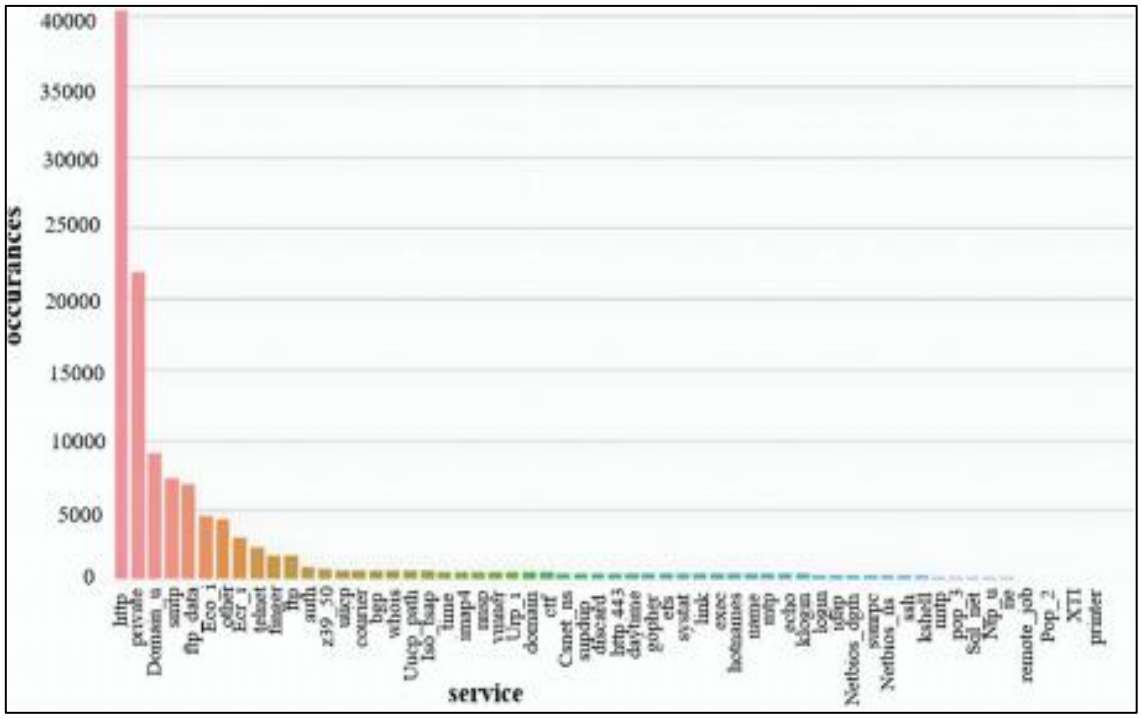

Fig 4: Features of NSL-KKD Dataset

A frequency distribution bar chart displaying several network services within the NSL-KDD dataset may be seen in Figure 4. It shows that certain services, such as http, smtp, domain_u, and ftp_data, occur far more frequently than others, while many services appear only a limited number of times. This imbalance underscores the importance of feature selection in focusing on the most informative services and minimizing the impact of rarely occurring features that may introduce noise rather than value.

Normalization

Several classifiers saw an improvement in their performance after pre-processing and data normalization to a score between 0 and 1 (Thomas, R., & Pavithran, D. 2018). The z-score regularization technique was used to normalize the attribute values. Once the data has been normalized, the standard deviation and mean are both set to 1.

Publisher: SARC Publisher

Data splitting

Dividing the NSL-KDD dataset in half could be an effective method to train and evaluate the proposed model. 70% of the data was used for training the hybrid LSTM-CNN model, while 30% was reserved for testing its classification accuracy. The 70-30 rule dictated the data divide.

Hybrid CNN-LSTM Model

A novel method for feature hybridization is provided by RNNs, which differ from conventional CNNs in that they aid in the creation of interactions between the input sequence. Figure 5 displays the results of researchers' efforts to hybridize features using LSTM, a type of RNN, which can improve recognition accuracy by sequentially extracting the long-term correlations of data attributes. Using multiple convolutional kernels, have developed a new but similar method of feature extraction in this work of the paper (Ahsan, M., & Nygard, K. E. 2020). Moreover, this strategy develops an overall map of the correlation between attributes and types of attacks. One part of the process uses CNNs to extract features, and the other part uses LSTMs to fuse those features. To create the forward propagation approach, one must first use a convolution layer to extract l and a pooling or extra input layer to extract l-1. The initial layer is determined using Equation (1):

$$xjl = f(\sum i \in Mjxil - 1 \times kij + bjl) \quad \text{Equation (1)}$$

The jth feature picture from the l layer is represented by xjl in the following equation. The activation function f(*), the difficulty process, and the total of all feature functions in the l-1 layer and the jth convolutional kernel of layer l are discussed in the section that follows. Afterwards, an offset parameter is included. This collection of variables includes the following: layer index (l), activation function (f), convolutional kernel (k), offset (b), and upper-layer input feature map (Mj). For convenience's sake, let's pretend that l is the down-sampling pooling layer and that l-1 is the convolution layer. Here is a breakdown of Equation (2).

$$xjl = f(\beta jldown(xjl - 1) + bjl \quad \text{Eq 2}$$

Convolutions and pooling are implemented using ReLU functions throughout the feature extraction stages. The baseline was 48 3x3 convolutional kernels. The LSTM processed 16 3x3 convolutional kernels using the max-pooling method, and the final output size was 70. The assault kinds are evaluated using the Softmax function.

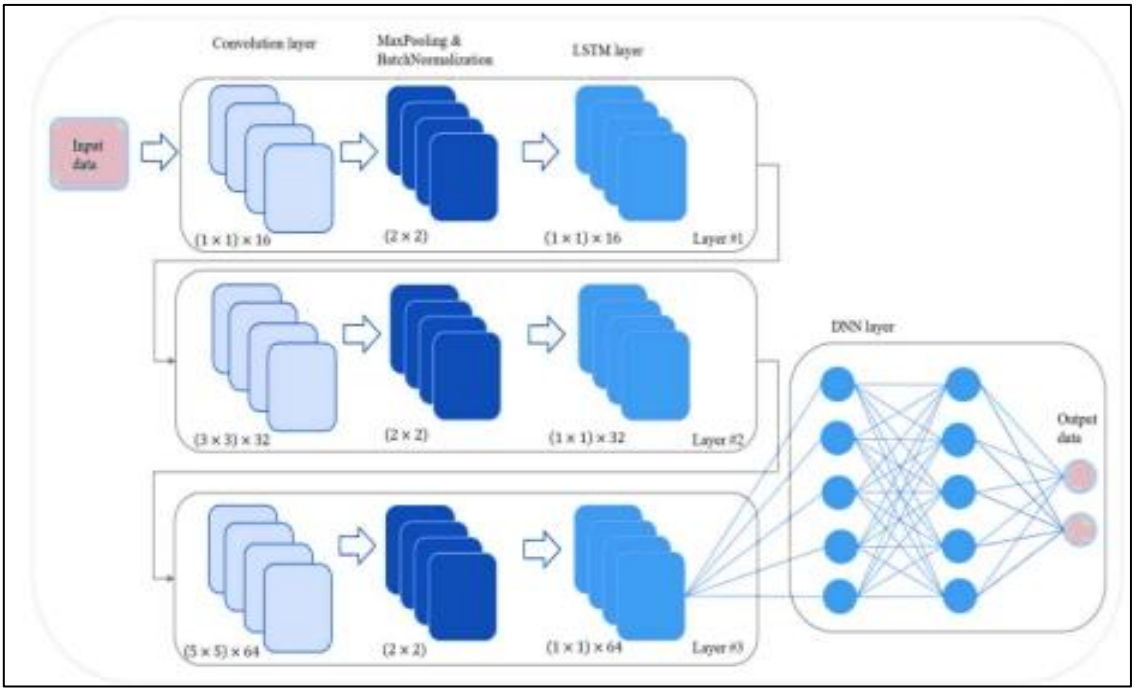

Fig 5: CNN-LSTM layer structure

Model Evaluation

A procedure for executing the planned mixture DL model on the NSL-KDD dataset's test subset (Sun, P. *et al.,* 2020). Ascertain the precision, F1 score, recall, and accuracy to evaluate the model's data categorization effectiveness. Detailed descriptions

Publisher: SARC Publisher

of the performance measures can be found below:

Accuracy

It is the gold standard by which all classification systems are evaluated. It explains how well a system can distinguish between legitimate and malicious connections. In Equation (3), it is expressed.

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN} \quad \text{(Equation 3)}$$

Recall

The real positive rate is another term for it. The proportion of correct results is determined using this statistic. Equation. (4) provides the derivation.

$$Recall = \frac{TP}{TP+FN} \quad \text{(Equation 4)}$$

Precision

One measure of the accuracy of a forecast model is the fraction of accurate class value predictions as a percentage of all successful forecasts. Here it is in Equation (5).

$$Precision = \frac{TP}{TP+FP} \quad \text{(Equation 5)}$$

F1-score

The F1-score is a metric for classifier performance, representing a weighted average of the two metrics, Recall and Precision. The description of Equation (6) follows.

$$F1 - Score = 2 * \frac{(Precision * Recall)}{Precision+Recall} \quad \text{(Equation 6)}$$

A correctly anticipated normal is denoted by TN, an incorrectly predicted attack is indicated by FP, an inaccurately predicted attack is shown by FN, a correctly predicted normal is indicated by TP, and so on.

Loss

The loss function is employed to quantify the extent to which the model deviates from its initial objectives during training. Because it is a performance metric for the model, this loss is optimized during training to minimize its value as much as possible. It is common practice to employ cross-entropy loss when dealing with attack classification and other multi-class classification problems.

RESULT ANALYSIS AND DISCUSSION

Windows 7, Intel Pentium (R), CPU G2020, and 2.90 GHz processor speeds were the bases for the experiments. Results for intrusion detection testing on the NSL-KDD dataset using the hybrid LSTM-CNN model are displayed in Table II. With a precision of 94.32%, the model proved its ability to reliably classify network traffic. It also attained a very high precision of 99.32%, indicating its effectiveness in minimizing false positives, while the recall value of 97.88% shows its robustness in correctly identifying actual attacks. A balanced performance in precision and recall, as shown by an F1 score of 98.60%, demonstrates the efficiency of the LSTM-CNN mixture structure in IDS trials.

Table 2: Experiment reulsts of hybrid models for instruiction detection system on nsl-kdd datset

Model	Accuracy	Precision	Recall	F1 Score
CNN-LSTM	94.32	99.32	97.88	98.60

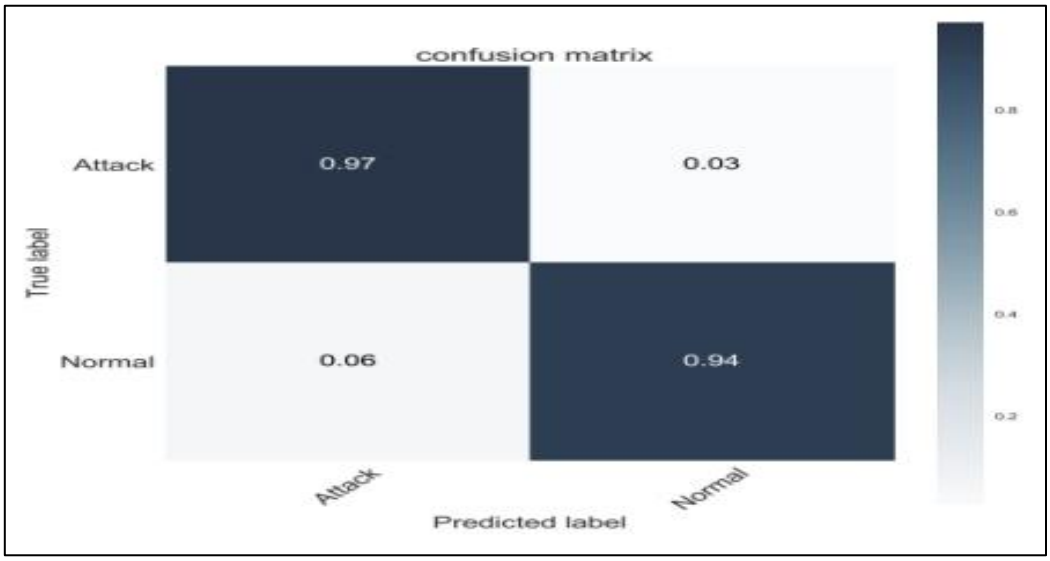

Figure 6: Binary Confusion Matrix for CNN-LSTM

Publisher: SARC Publisher

Figure 6 displays the confusion matrix of the LSTM-CNN model on the NSL-KDD dataset. The model's exceptional classification capacity is fully on display, with a 97% accuracy rate in detecting assaults and a 94% accuracy rate in identifying normal cases. Reliably distinguishing between harmful and benign traffic, the model continues to have low misclassification rates with only 3% of FN and 6% of FP.

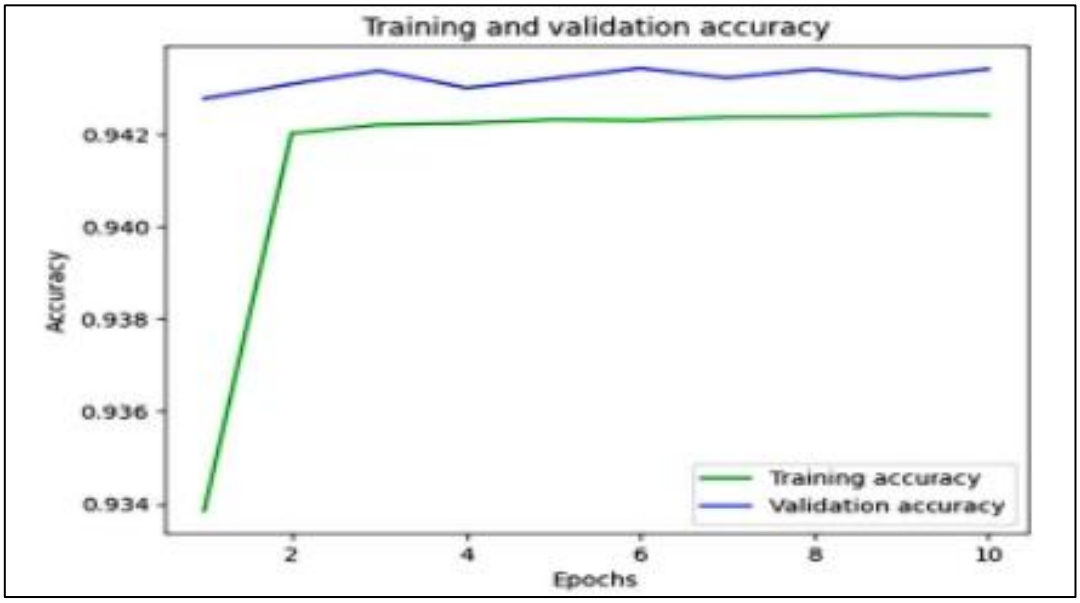

Fig 7: Loss Curve for CNN-LSTM Hybrid Model

Training and Validation Accuracy of CNN-LSTM Model

Figure 7 displays the LSTM-CNN model's validation and training accuracy curves for a total of 10 epochs. The curves exhibit rapid convergence during the initial two epochs and then stabilize at high levels. A lack of overfitting and good generalization are both confirmed by the fact that the proof accuracy is marginally higher than the training accuracy.

Figure 8 displays the loss arc for LSTM-CNN hybrid model across 10 training epochs. Separate lines representing the training loss (green) and validation loss (blue) are displayed on the graph, which shows the loss (y-axis) plotted against the number of epochs (x-axis). Training and validation loss both drop dramatically in the early epochs of the plot, which means that learning is going well. The loss numbers start to level out and get closer together after the second epoch. Particularly, the validation loss consistently falls below the training loss.

Comparative Analysis

The results of various models for detecting intrusions in networks are compared in Table III. The usefulness of the hybrid CNN-LSTM model in identifying intrusions is demonstrated by its maximum accuracy (94.32%), precision (99.32%), recall (97.88%), and F1 score (98.60%), which surpasses the standard techniques. In contrast, LR achieves an accuracy of 74.37% and a recall of 60.01%, while SVM shows the lowest performance with 68% accuracy, 68.35% precision, and 65.15% recall. These outcomes demonstrate that, when contrasted with conventional ML methods, the CNN-LSTM hybrid model performs superiorly in terms of accurate and dependable network traffic categorization.

Table 3: Model Performance Comparison of Network Intrusion Detection for Cybersecurity

Model	Accuracy	Precision	Recall	F1 Score
CNN-LSTM	94.32	99.32	97.88	98.60
LR(Gupta, G. P., & Kulariya, M. 2016)	74.37	-	60.01	98.34
SVM(Khan, M. A. *et al.*, 2019)	68	68.35	65.15	67.86

The hybrid CNN-LSTM model, suggested, possesses a better network intrusion detection up to the 94.32-99.32% of accuracy, on the NSL-KDD set. Even complex traffic patterns can be easily derived to create features using CNN and the sequential interactions can be learned using LSTM leading to high accuracies and decreased errors. The remaining strength of this model is that

Publisher: SARC Publisher

it exhibits good generalization ability, as shown by the stable validation results, and is resistant to both false positives and false negatives. That is why the LSTM method is very efficient and valid compared to traditional ML approaches for improving cybersecurity.

CONCLUSION AND FUTURE SCOPE

In the digital age, hacking remains a significant problem because malicious activities continue to escalate in complexity, posing a threat to the privacy, security, and availability of critical systems. Presenting a hybrid IDS that combines CNN and LSTM, this research. It would use the NSL-KDD dataset to be more resistant to a lot of intrusions. The experimental findings revealed that CNN-LSTM outperformed traditional algorithms, including LR and SVM, with a recall of 97.88%, precision of 99.32%, and F1-score of 98.60%, achieving an accuracy of 94.32%. The high accuracy in validation and the low cases of misclassification indicate that the model has a great generalization ability and can effectively classify normal and malicious traffic. The study is limited despite the impressive findings. This model was also only tested using the NSL-KDD dataset, which is not a complete representation of current network traffic or contemporary attack techniques. Additionally, data imbalance is an issue that is especially evident in the detection of uncommon attacks, such as U2R and R2L, where speed can be compromised.

For future work, it would be beneficial to test on new datasets such as CIC-IDS2017 or UNSW-NB15. To address class imbalance, one can use generative methods such as SMOTE or GAN-based augmentation. Attention mechanisms or transformer-based models could be added to detect long-term dependencies and subtle attack patterns.

REFERENCES

1. Abubakar, A. I., Chiroma, H., Muaz, S. A., & Ila, L. B. "A review of the advances in cyber security benchmark datasets for evaluating data-driven based intrusion detection systems." *Procedia Computer Science* 62 (2015): 221-227.
2. Sarker, I. H., Abushark, Y. B., Alsolami, F., & Khan, A. I. "Intrudtree: a machine learning based cyber security intrusion detection model." *Symmetry* 12.5 (2020): 754.
3. Liu, G., & Zhang, J. "CNID: research of network intrusion detection based on convolutional neural network." *Discrete Dynamics in Nature and Society* 2020.1 (2020): 4705982.
4. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study." *Journal of Information Security and Applications* 50 (2020): 102419.
5. Kushwaha, A., Pathak, P., & Gupta, S. "Review of Optimize Load Balancing Algorithms in Cloud." *International Journal of Distributed & Cloud Computing* 4.2 (2016).
6. Liu, H., & Lang, B. "Machine learning and deep learning methods for intrusion detection systems: A survey." *applied sciences* 9.20 (2019): 4396.
7. Maddali, G. "Zero Trust Security Architectures for Large-Scale Cloud Workloads." *Available at SSRN 5365222* (2025).
8. Thapliyal, A., Bhagavathi, P. S., Arunan, T., & Rao, D. D. "Realizing zones using UPnP." *2009 6th IEEE Consumer Communications and Networking Conference*. IEEE, (2009).
9. Neeli, S. S. S. "Serverless Databases: A Cost-Effective and Scalable Solution." *Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci* 7.6 (2019): 7.
10. Buczak, A. L., & Guven, E. "A survey of data mining and machine learning methods for cyber security intrusion detection." *IEEE Communications surveys & tutorials* 18.2 (2015): 1153-1176.
11. H. P. Kapadia, "Cross-Platform UI/UX Adaptions Engine for Hybrid Mobile Apps," *Int. J. Nov. Res. Dev.*, vol. 5, no. 9, pp. 30–37, (2020).
12. Neeli, S. S. S. "The Significance of NoSQL Databases: Strategic Business Approaches and Management Techniques." *J. Adv. Dev. Res* 10.1 (2019): 11.
13. Karanam, L., Pattanaik, K. K., & Aldmour, R. "Intrusion detection mechanism for large scale networks using CNN-LSTM." *2020 13th International Conference on Developments in eSystems Engineering (DeSE)*. IEEE, (2020).
14. BACHAR, A., EL MAKHFI, N., & Bannay, O. E. "Towards a behavioral network intrusion detection system based on the SVM model." *2020 1st International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)*. IEEE, (2020).
15. Latif, S., Idrees, Z., Zou, Z., & Ahmad, J. "DRaNN: A deep random neural network model for intrusion detection in industrial

Publisher: SARC Publisher

IoT." *2020 international conference on UK-China emerging technologies (UCET)*. IEEE, (2020).
16. Khan, R. U., Zhang, X., Alazab, M., & Kumar, R. "An improved convolutional neural network model for intrusion detection in networks." *2019 Cybersecurity and cyberforensics conference (CCC)*. IEEE, (2019).
17. Zhiqiang, L., Mohi-Ud-Din, G., Bing, L., Jianchao, L., Ye, Z., & Zhijun, L. "Modeling network intrusion detection system using feed-forward neural network using unsw-nb15 dataset." *2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE)*. IEEE, (2019).
18. Srivastava, A., Agarwal, A., & Kaur, G. "Novel Machine Learning Technique for Intrusion Detection in Recent Network-based Attacks." *2019 4th International Conference on Information Systems and Computer Networks (ISCON)*. IEEE, (2019).
19. Larijani, H., Ahmad, J., & Mtetwa, N. "A novel random neural network based approach for intrusion detection systems." *2018 10th Computer Science and Electronic Engineering (CEEC)*. IEEE, (2018).
20. Thomas, R., & Pavithran, D. "A survey of intrusion detection models based on NSL-KDD data set." *2018 Fifth HCT Information Technology Trends (ITT)* (2018): 286-291.
21. Ahsan, M., & Nygard, K. E. "Convolutional Neural Networks with LSTM for Intrusion Detection." *CATA*. Vol. 69. (2020).
22. Sun, P., Liu, P., Li, Q., Liu, C., Lu, X., Hao, R., & Chen, J. "DL-IDS: Extracting Features Using CNN-LSTM Hybrid Network for Intrusion Detection System." *Security and communication networks* 2020.1 (2020): 8890306.
23. Gupta, G. P., & Kulariya, M. "A framework for fast and efficient cyber security network intrusion detection using apache spark." *Procedia Computer Science* 93 (2016): 824-831.
24. Khan, M. A., Karim, M. R., & Kim, Y. "A scalable and hybrid intrusion detection system based on the convolutional-LSTM network." *Symmetry* 11.4 (2019): 583.
25. Polam, R. M., Kamarthapu, B., Kakani, A. B., Nandiraju, S. K. K., Chundru, S. K., & Vangala, S. R. "Big Text Data Analysis for Sentiment Classification in Product Reviews Using Advanced Large Language Models." *International Journal of AI, BigData, Computational and Management Studies* 2.2 (2021): 55-65.
26. Gangineni, V. N., Tyagadurgam, M. S. V., Chalasani, R., Bhumireddy, J. R., & Penmetsa, M. "Strengthening Cybersecurity Governance: The Impact of Firewalls on Risk Management." *International Journal of AI, BigData, Computational and Management Studies* 2 (2021): 10-63282.
27. Pabbineedi, S., Penmetsa, M., Bhumireddy, J. R., Chalasani, R., Tyagadurgam, M. S. V., & Gangineni, V. N. "An Advanced Machine Learning Models Design for Fraud Identification in Healthcare Insurance." *International Journal of Artificial Intelligence, Data Science, and Machine Learning* 2.1 (2021): 26-34.
28. Kamarthapu, B., Kakani, A. B., Nandiraju, S. K. K., Chundru, S. K., Vangala, S. R., & Polam, R. M. "Advanced Machine Learning Models for Detecting and Classifying Financial Fraud in Big Data-Driven." *International Journal of Artificial Intelligence, Data Science, and Machine Learning* 2.3 (2021): 39-46.
29. Tyagadurgam, M. S. V., Gangineni, V. N., Pabbineedi, S., Penmetsa, M., Bhumireddy, J. R., & Chalasani, R. "Enhancing IoT (Internet of Things) Security Through Intelligent Intrusion Detection Using ML Models." *International Journal of Emerging Research in Engineering and Technology* 2.1 (2021): 27-36.
30. Vangala, S. R., Polam, R. M., Kamarthapu, B., Kakani, A. B., Nandiraju, S. K. K., & Chundru, S. K. "Smart Healthcare: Machine Learning-Based Classification of Epileptic Seizure Disease Using EEG Signal Analysis." *International Journal of Emerging Research in Engineering and Technology* 2.3 (2021): 61-70.
31. Kakani, A. B., Nandiraju, S. K. K., Chundru, S. K., Vangala, S. R., Polam, R. M., and Kamarthapu, B. "Big Data and Predictive Analytics for Customer Retention: Exploring the Role of Machine Learning in E-Commerce." *International Journal of Emerging Trends in Computer Science and Information Technology* 2.2 (2021): 26–34.
32. Penmetsa, M., Bhumireddy, J. R., Chalasani, R., Tyagadurgam, M. S. V., Gangineni, V. N., and Pabbineedi, S. "Next-Generation Cybersecurity: The Role of AI and Quantum Computing in Threat Detection." *International Journal of Emerging Trends in Computer*

Publisher: SARC Publisher

Science and Information Technology 2.4 (2021): 54–61.
33. Polu, A. R., Vattikonda, N., Gupta, A., Patchipulusu, H., Buddula, D. V. K. R., and Narra, B. "Enhancing Marketing Analytics in Online Retailing through Machine Learning Classification Techniques." *Available at SSRN* 5297803 (2021).
34. Polu, A. R., Buddula, D. V. K. R., Narra, B., Gupta, A., Vattikonda, N., and Patchipulusu, H. "Evolution of AI in Software Development and Cybersecurity: Unifying Automation, Innovation, and Protection in the Digital Age." *Available at SSRN* 5266517 (2021).
35. Polu, A. R., Vattikonda, N., Buddula, D. V. K. R., Narra, B., Patchipulusu, H., and Gupta, A. "Integrating AI-Based Sentiment Analysis With Social Media Data for Enhanced Marketing Insights." *Available at SSRN* 5266555 (2021).
36. Buddula, D. V. K. R., Patchipulusu, H. H. S., Polu, A. R., Vattikonda, N., and Gupta, A. K. "Integrating AI-Based Sentiment Analysis with Social Media Data for Enhanced Marketing Insights." *International Journal of Engineering Science and Management* 10.2 (2021).
37. Gupta, A. K., Buddula, D. V. K. R., Patchipulusu, H. H. S., Polu, A. R., Narra, B., and Vattikonda, N. "An Analysis of Crime Prediction and Classification Using Data Mining Techniques." *Unpublished manuscript* (2021).
38. Rajiv, C., Mukund Sai, V. T., Venkataswamy Naidu, G., Sriram, P., and Mitra, P. "Leveraging Big Datasets for Machine Learning-Based Anomaly Detection in Cybersecurity Network Traffic." *Journal of Contemporary Education Theory and Artificial Intelligence (JCETAI)* (2022): 102.
39. Sandeep Kumar, C., Srikanth Reddy, V., Ram Mohan, P., Bhavana, K., and Ajay Babu, K. "Efficient Machine Learning Approaches for Intrusion Identification of DDoS Attacks in Cloud Networks." *Journal of Contemporary Education Theory and Artificial Intelligence (JCETAI)* (2022): 101.
40. Bhumireddy, J. R., Chalasani, R., Tyagadurgam, M. S. V., Gangineni, V. N., Pabbineedi, S., and Penmetsa, M. "Big Data-Driven Time Series Forecasting for Financial Market Prediction: Deep Learning Models." *Journal of Artificial Intelligence and Big Data* 2.1 (2020): 153–164. DOI: 10.31586/jaibd.2022.1341.
41. Nandiraju, S. K. K., Chundru, S. K., Vangala, S. R., Polam, R. M., Kamarthapu, B., and Kakani, A. B. "Advance of AI-Based Predictive Models for Diagnosis of Alzheimer's Disease (AD) in Healthcare." *Journal of Artificial Intelligence and Big Data* 2.1 (2022): 141–152. DOI: 10.31586/jaibd.2022.1340.
42. Tyagadurgam, M. S. V., Gangineni, V. N., Pabbineedi, S., Penmetsa, M., Bhumireddy, J. R., and Chalasani, R. "Designing an Intelligent Cybersecurity Intrusion Identify Framework Using Advanced Machine Learning Models in Cloud Computing." *Universal Library of Engineering Technology* (2022).
43. Vangala, S. R., Polam, R. M., Kamarthapu, B., Kakani, A. B., Nandiraju, S. K. K., and Chundru, S. K. "Leveraging Artificial Intelligence Algorithms for Risk Prediction in Life Insurance Service Industry." *Available at SSRN* 5459694 (2022).
44. Polam, R. M., Kamarthapu, B., Kakani, A. B., Nandiraju, S. K. K., Chundru, S. K., and Vangala, S. R. "Data Security in Cloud Computing: Encryption, Zero Trust, and Homomorphic Encryption." *International Journal of Emerging Trends in Computer Science and Information Technology* 2.3 (2021): 70–80.
45. Gangineni, V. N., Pabbineedi, S., Penmetsa, M., Bhumireddy, J. R., Chalasani, R., and Tyagadurgam, M. S. V. "Efficient Framework for Forecasting Auto Insurance Claims Utilizing Machine Learning Based Data-Driven Methodologies." *International Research Journal of Economics and Management Studies (IRJEMS)* 1.2 (2021).
46. Vattikonda, N., Gupta, A. K., Polu, A. R., Narra, B., Buddula, D. V. K. R., and Patchipulusu, H. H. S. "Blockchain Technology in Supply Chain and Logistics: A Comprehensive Review of Applications, Challenges, and Innovations." *International Journal of Emerging Research in Engineering and Technology* 3.3 (2022): 99–107.
47. Narra, B., Vattikonda, N., Gupta, A. K., Buddula, D. V. K. R., Patchipulusu, H. H. S., and Polu, A. R. "Revolutionizing Marketing Analytics: A Data-Driven Machine Learning Framework for Churn Prediction." *International Journal of Artificial Intelligence, Data Science, and Machine Learning* 3.2 (2022): 112–121.
48. Polu, A. R., Narra, B., Buddula, D. V. K. R., Patchipulusu, H. H. S., Vattikonda, N., and

Publisher: SARC Publisher

Gupta, A. K. "Blockchain Technology as a Tool for Cybersecurity: Strengths, Weaknesses, and Potential Applications." *Unpublished manuscript* (2022).

49. Bhumireddy, J. R., Chalasani, R., Tyagadurgam, M. S. V., Gangineni, V. N., Pabbineedi, S., and Penmetsa, M. "Big Data-Driven Time Series Forecasting for Financial Market Prediction: Deep Learning Models." *Journal of Artificial Intelligence and Big Data* 2.1 (2022): 153–164. DOI: 10.31586/jaibd.2022.1341.
50. Nandiraju, S. K. K., Chundru, S. K., Vangala, S. R., Polam, R. M., Kamarthapu, B., and Kakani, A. B. "Advance of AI-Based Predictive Models for Diagnosis of Alzheimer's Disease (AD) in Healthcare." *Journal of Artificial Intelligence and Big Data* 2.1 (2022): 141–152. DOI: 10.31586/jaibd.2022.1340.

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:

Rajendran, D., Maniar, V., Tamilmani, V., Namburi, V. D., Singh, A. A. S. and Kothamaram, R. R. " CNN-LSTM Hybrid Architecture for Accurate Network Intrusion Detection for Cybersecurity." *Sarcouncil Journal of Engineering and Computer Sciences* 2.11 (2023): pp 1-13.

Publisher: SARC Publisher