International Journal of Advanced and Applied Sciences

Journal homepage: http://www.ijaas.in

An Investigation the ML\DL Hybrid Model for Social Media Attack Prediction and Detection

Rashmi Tiwari [1*], Dr. Gaurav Aggarwal [2]

[1] *Research Scholar, Faculty of Engineering & Technology, Jagannath University, Jhajjar, India*
[2] *Professor, Faculty of Engineering & Technology, Jagannath University, Jhajjar, India*

ARTICLE INFO

Article history:
Received: 12-05-2025
Received in revised form: 08-06-2025
Accepted: 12-07-2025

Keywords:

Social media security, Cyber-attack detection, Machine learning, Deep learning, Hybrid models, CNN, LSTM, GRU, Autoencoder, Intrusion prediction

ABSTRACT

The proliferation of social media platforms has increased the risk of cyber-attacks, necessitating advanced techniques for timely detection and prevention. This study investigates the application of hybrid Machine Learning (ML) and Deep Learning (DL) models for social media attack prediction and detection. By integrating ML's ability to extract salient features with DL's strength in modeling complex temporal and spatial patterns, hybrid models demonstrate enhanced accuracy and robustness in identifying malicious activities. The research examines various architectures, including CNNs, LSTMs, GRUs, and autoencoders, highlighting their effectiveness in handling high-dimensional, imbalanced, and dynamic social media data. The findings underscore the potential of ML/DL hybrid frameworks to provide real-time, adaptive, and reliable solutions for mitigating cyber threats, ultimately contributing to safer online communication environments.

Introduction

Ensuring the security of networks is becoming increasingly important as more damaging attacks emerge every year. Hackers and other malicious actors use ingenious methods, such as hybrid attacks, to compromise network security. To bolster network security against such attacks, Intrusion Detection System (IDS) is a popular solution. Intrusions and other anomalies that compromise the integrity, confidentiality, or accessibility of computer networks are detected at the network level using a (NIDS). Some of the earlier solutions for NIDS were implemented using other conventional methods, such as signature matching, which give unsatisfactory results in predicting the highly complex network data [1]. Popular Machine Learning (ML) algorithms, including Random Forest (RF), Support Vector Machine (SVM), Decision Trees (DT), etc., have been applied to widely used, up-to-date datasets. However, with the increasing diversity and complexity of

cyber-attacks, these ML models often struggle to accurately capture the behavioural patterns of various attack classes, particularly within imbalanced datasets. This limitation affects their efficacy in identifying emerging and sophisticated threats, indicating the need for enhanced feature engineering, hybrid models, or advanced tuning approaches to improve detection capabilities against evolving attack vectors.

With the performance of ML models reaching a plateau and the increasing availability of GPU power, deep learning models have gained in popularity [2]. Deep learning models offer much superior performance when compared to ML methods. Popular deep learning algorithms like CNN and Recurrent Neural Networks (RNN) have consistently predicted different attack classes. While the average accuracy of the models has steadily increased year after year, most of the NIDS solutions still suffer from a high False Alarm Rate (FAR) and poor Detection Rate (DR).

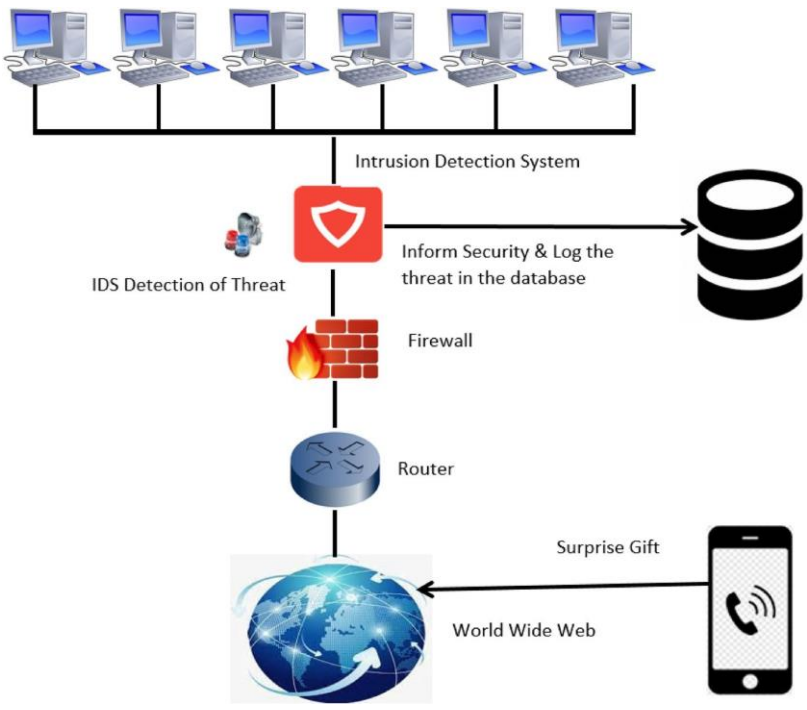

Figure 1: Intrusion Detection System in General

Currently, several research works have focused on building multistage models using two or more deep-learning models in a pipeline. Recent multi-stage sequential models such as Seq2Seq are popular in fields like Natural Language Processing (NLP) and can be further explored to develop NIDS. These Sequential deep learning algorithms generally model the temporal nature of the network data more effectively. There is scope to improve the quality of predictions using innovative methods in deep learning with more effective spatial and temporal feature extraction that can help to reduce FAR and improve DR. This paper proposes a hybrid deep-learning NIDS model that integrates Conv LSTM sub- nets within the Seq2Seq architecture. This design choice aims to enhance the quality of spatial and temporal representations, ultimately contributing to more effective model building. This approach minimizes manual biases, ensuring an efficient and unbiased extraction of significant dependencies from the input data. These extracted representations are utilized in the Seq2Seq autoencoder structure, which has shown promising results in making high-accuracy predictions and addressing class imbalance issues.

To validate the adaptability of the proposed model, we evaluate its performance on multiple datasets, including CIC-IDS2017, CIC-ToN-IoT, and UNSW-NB15. We further enhance model interpretability by employing LIME, the XAI technique. Explainable AI refers to methods that make machine learning models more transparent and interpretable, allowing users to understand and trust model decisions [3]. LIME explains individual predictions by approximating the complex model with a simpler, interpretable model for specific instances. An IDS needs to be smart and efficient at identifying and stopping both known and unidentified threats, like anomaly detection, to protect these networks The applications of artificial intelligence (AI) to NIDS have become the subject of recent research, and AI-based intrusion detection systems have demonstrated incredible performance. Initially, the primary goal is to integrate well- known machine learning models such as Decision Tree (DT) and Support Vector Machine (SVM) into intrusion detection systems to incorporate deep learning methods like CNNs, LSTMs, and autoencoders. Despite the impressive performance, these results have shown in identifying abnormalities, which also

presents issues related to applying them to actual systems.

Table 1: Binary & Multiclass Classification

Dataset	Binary			Multiclass	
	No of records	Records type		No of records	Records type
WSN-DS	2	Normal or Attack		10	Black hole, Gray hole
NSL-KDD	2	Normal or Attack		5	DoS, U2R, Probe, and R2L
UNSW-NB15	2	Normal or Attack		9	Shell code, Backdoor, Generic
CIC-IDS 2017	2	Normal or Attack		7	Normal, Bot, Brute Force

The authors of developed a hybrid intrusion detection model in research for cloud-based systems that can identify all kinds of attacks by combining anomaly and signature-based detection. In another study, the authors of to detect attacks, suggested a novel two-stage deep learning technique that hybridizes long-short-term memory (LSTM) and auto-encoders (AE).

Deep learning uses ANN algorithms for machine learning, making it hierarchical. Assaults are identified using 1D-CNN, a unique form of convolutional neural networks, which classifies traffic into normal and attack data (CNN). When real-world data increases over time, generating a high- dimensional space, the performance of ML algorithms declines because these techniques rely too much on the qualities chosen by human experts. By automatically learning features from a massive amount of data, DL was able to circumvent this limitation, thanks to its complex architecture. In this study, we propose a 1D-CNN & LSTM hybrid neural network for social media assault prediction [4]. This reduces the overall efficacy of NIDS and makes it harder to detect particular types of attacks. Even though inconsistent data negatively affects NIDS's ability to detect assaults, this problem has not gotten enough attention in recent NIDS studies.

The current study builds a hybrid intrusion detection classification model based on ML and DL in combination to increase the detection rate (DR) and accuracy. The datasets cover all potential attack methods in the context of Indus experimental IoT and contain rich sample sizes.

Literature review

Akhtar, M. S., & Feng, T. (2022) [1] focus on real-time malware detection using a hybrid deep learning approach combining Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. The study demonstrates that the CNN component effectively extracts spatial features from malware data, while the LSTM captures temporal dependencies, resulting in improved detection accuracy. The authors highlight the efficiency of this model in real-time scenarios, emphasizing its potential to enhance cybersecurity measures against evolving malware threats. This research contributes to the field by integrating spatial and temporal feature learning into a single framework for robust malware detection.

Liu, Y., Wang, X. K., Hou, W. H., Liu, H., & Wang, J. Q. (2022) [2] propose a novel hybrid model combining a fuzzy inference system with deep learning for short-term traffic flow prediction. The fuzzy inference system addresses uncertainties and vagueness in traffic data, while deep learning captures complex temporal patterns. Their results indicate that this hybrid approach significantly improves prediction accuracy compared to traditional models. The study underscores the value of integrating domain knowledge with data-driven deep learning techniques to handle dynamic and uncertain systems such as urban traffic networks.

Mahajan, S., HariKrishnan, R., & Kotecha, K. (2022) [3] investigate network traffic prediction in wireless mesh networks using a hybrid deep learning model. By combining multiple neural network architectures, the model captures both spatial and temporal dependencies in network traffic patterns. The study demonstrates improved predictive performance and efficiency, which can optimize network management and resource allocation. This research highlights the applicability of hybrid deep learning techniques in wireless communication systems to enhance performance and reliability.

Petmezas, G., Haris, K., Stefanopoulos, L., Kilintzis, V., Tzavelis, A., Rogers, J. A., ... & Maglaveras, N. (2021) [4] develop a hybrid CNN-LSTM network for automated atrial fibrillation detection on highly imbalanced ECG datasets. The CNN extracts local temporal features from ECG signals, while LSTM captures long-term dependencies, improving detection performance even with imbalanced classes. The study emphasizes that the hybrid approach outperforms conventional methods and provides reliable real-time detection of cardiac arrhythmias. This work illustrates the potential of hybrid deep learning frameworks in critical healthcare applications.

Rizvi, S., Scanlon, M., McGibney, J., & Sheppard, J. (2022) [5] present a deep learning-based network intrusion detection system designed for resource-constrained environments. The study employs lightweight neural network architectures to ensure high detection accuracy while maintaining computational efficiency. Their results demonstrate that deep learning can effectively identify complex intrusion patterns even in environments with limited hardware capabilities. This research contributes to practical cybersecurity solutions by adapting advanced machine learning methods for deployment in constrained systems.

Sasidhar, T. T., Premjith, B., & Soman, K. P. (2020) [6] focus on emotion detection in code-mixed social media text, specifically Hinglish (Hindi + English). The study proposes a machine learning-based approach to identify emotional states from informal and mixed-language posts, addressing challenges posed by language blending, slang, and contextual nuances. Their results indicate that tailored feature extraction and language-specific preprocessing significantly enhance detection accuracy. This research contributes to natural language processing by providing methods to handle code-mixed texts, which are increasingly prevalent in social media analytics.

Satyanegara, H. H., & Ramli, K. (2022) [7] investigate the implementation of hybrid deep learning models, specifically CNN-MLP and CNN-LSTM, for detecting Man-in-the-Middle (MitM) attacks in network systems. Their study demonstrates that combining convolutional networks for feature extraction with either multilayer perceptrons or LSTMs for classification improves detection performance over traditional methods. The research highlights the effectiveness of hybrid models in

identifying sophisticated network intrusions and reinforces the potential of deep learning in cyber security.

Song, Z. (2020) [8] explores English speech recognition using deep learning models that incorporate multiple acoustic and linguistic features. The study emphasizes the importance of feature diversity, including spectral, temporal, and prosodic information, in improving recognition accuracy. Results show that integrating multiple feature sets with deep neural architectures leads to robust speech recognition even in noisy environments. This work contributes to the development of advanced speech processing systems and demonstrates the adaptability of deep learning to complex audio tasks.

Tian, C., Fei, L., Zheng, W., Xu, Y., Zuo, W., & Lin, C.-W. (2020) [9] provide a comprehensive overview of deep learning approaches for image denoising. The study reviews various architectures, including CNNs, autoencoders, and generative models, highlighting their strengths in removing noise while preserving image details. The authors discuss both supervised and unsupervised strategies and identify challenges such as computational cost and generalization across noise types. This work serves as a foundational reference for researchers applying deep learning to image enhancement and computer vision tasks.

Hussain, J., & Hnamte, V. (2021) [10] present a modern deep learning-based intrusion detection system for cyber security applications. Their study focuses on leveraging neural network architectures to detect complex attack patterns in network traffic. Results indicate that deep learning models can significantly outperform conventional intrusion detection systems in terms of accuracy and adaptability to evolving threats. The research emphasizes the importance of continuous model training and feature optimization to enhance real-time detection capabilities.

Nasreen Fathima, A. H., & Ibrahim, S. P. S. (2022) [11] propose a multi-stage deep investigation pipeline to detect malign network traffic. The study integrates layered deep learning mechanisms to sequentially analyze network data, enabling early identification of suspicious patterns and mitigating false positives. The approach demonstrates improved detection accuracy for complex and evolving cyber threats, emphasizing the effectiveness of multi-stage pipelines in handling high-dimensional and dynamic network traffic. This research

contributes to the advancement of real-time cyber security solutions by combining precision and computational efficiency.

Jerusha, Y. A., Ibrahim, S. P. S., & Varadharajan, V. (2023) [12] develop an effective network intrusion detection model that classifies attacks from coarse to fine granularity in imbalanced network traffic datasets. The model addresses challenges associated with unequal class distributions, employing deep learning techniques to accurately distinguish between major and subtle attack types. The findings reveal that hierarchical classification significantly enhances detection performance while reducing misclassification rates. This study underscores the importance of designing intrusion detection systems capable of handling imbalanced and complex network environments.

Methodology

Recent advances in cyber security research for constructing high-performance NIDS indicate that integrating components from multiple models and refining their architectures can lead to significant performance improvements [4]. We see potential for enhancing feature extraction by incorporating a spatial dimension into the learning process. Convolutional operations are particularly not well-suited for capturing high- level features and spatial dependencies. We optimized the learning process to ensure that our proposed Conv LSTM module enables synchronous learning of spatial and temporal components. This design choice is inspired by the success of prior work Lu NET which demonstrated the effectiveness of synchronous training compared to pipeline- based approaches [5]. To the best of our knowledge, Conv LSTM has not yet been applied for anomaly detection, particularly within the domain of NIDS research, which represents a novel area of exploration. Moreover, advancements in XAI have substantially improved the interpretability and reliability of machine learning models in NIDS.

Recent advances in machine learning have elevated NIDS to essential tools for detecting malicious activities in network environments. Modern NIDS must analyze increasingly complex data patterns to identify spatial and temporal threats. Traditional NIDS models, such as signature-based systems, often suffer from high false positive rates and fail to detect novel or zero-day attacks due to their inability to capture intricate dependencies within network data. While recent deep learning-based NIDS models have improved

behavioural pattern analysis, challenges remain, particularly in capturing long-range temporal dependencies and processing high-dimensional data from diverse sources. This research focuses on developing a hybrid DL model to address network attacks by analyzing long-term attack behaviours. Enhancing the quality of temporal and spatial dependencies learned by the model is central to improving algorithm performance. Although various deep learning methods are available for NIDS, the Seq2Seq architecture has demonstrated superior predictive accuracy, making it the foundation of our proposed approach. A Seq2Seq model is a type of neural network architecture beneficial for tasks where the input and output are sequences of different lengths [6].

It takes the input in the form of a vector sequence $I = (i_1, i_2, \ldots, i_t)$, where t is the time variable. The output from the encoder is obtained from the last LSTM cell in the sequence and can be denoted by the fixed vector v = activation $(f_1, f_2, \ldots, f_t)$. f_i, and the chosen non-linear activation function is applied over the vector. The decoder produces a sequence of predictions $p = (p_1, p_2, \ldots, p_t)$ corresponding to the time variable t. We designed a hybrid Seq2Seq model that enhances traditional architectures by replacing the LSTM core with Conv LSTM units. By leveraging the strengths of CNNs for spatial feature extraction and LSTMs for temporal sequence modeling Conv LSTM units allow the model to handle spatiotemporal data, with improved generalization.

The intrusion detection system gathers and examines security logs, audit data, network behavior, and other network available information. It also makes numerous crucial systemic inferences [7]. It looks for indications that the network or system is under attack as well as whether certain actions are against security policies. displays the general intrusion detection model diagram where it can be seen that the attack has occurred and the intrusion detection system captured the attack and stored it in log files for further actions. The basic intrusion detection model serves as the foundation for the approach put forth in this work. To avoid waiting for the session to end and to reduce the time needed to construct the session feature, it is crucial to employ packet data directly as a feature to achieve real-time detection. The flowchart for the hybrid model finding a packet that can reliably distinguish if an intrusion has happened and detecting the network intrusion based on it are both required at the same

time. Current studies are unable to offer this capacity. During the data preparation process, the data ranges are changed to improve the compilation and application of the knowledge in a specific dataset. There is a notable contrast shift between the dataset's maximum and lowest range. Data normalization facilitates an approach by reducing the difficulties involved in this process. When applying neural network classification techniques, data normalization has a greater influence [8]. If the neural network learns a back propagation strategy, input normalization will cause it to speed up training at this point, it will reach maximum efficiency.

Scaling

The normalization of the Americanized data and the differences in the standard deviations and average values of the data read from the CSV file will impact the effectiveness of the learning process. The input data was scaled with Standard Scalar, yielding a standard deviation of one and a mean of zero. Datasets are normalized using library standard scalars by sk learn preprocessing.

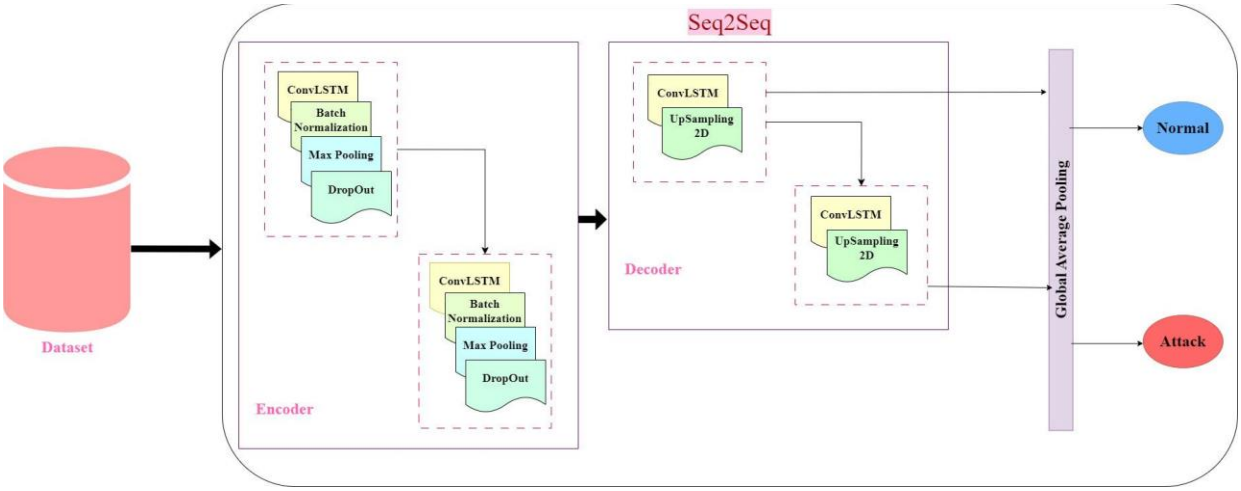

FIGURE 2: Proposed hybrid Seq2Seq and Conv LSTM model for NIDS

Regularization technique

L2 regularization is used to determine how comparable the two samples are and the model does not over fit during training. The primary uses of this technique are in text clustering and classification. L2 regularization was chosen because it can highlight certain features with a lesser

value but greater significance and weaken the strong features as much as feasible.

The study of research methodology is a branch of the scientific community. It is a method for methodically resolving the research issue [9]. An organized plan outlining the procedures to be followed in conducting the research has been prepared as part of the research design for the study. This research is a descriptive empirical survey.

Data Collection

The researcher has used different sets of data collection techniques to have comprehensive and desired information. The nature of the study demanded that the researcher should collect data from various reliable sources. The researcher has used and relied on both the primary and secondary sources of data collection.

Primary Data

Primary data consists of information gathered directly by the researcher. You can trust it more since it is genuine. Questions, interviews, observations, and the provision of schedules are all viable methods for its acquisition. The researcher in this study gathered primary data through the use of questionnaires.

Secondary Data

The primary researcher may make use of secondary data, which consists of information gathered from other sources such as agencies and studies. Academic journals, vernacular news studies, annual reports, government reports, and trustworthy websites are the sources from which it is compiled. Secondary data gathered from a variety of sources is utilized in this research For the purpose of minimizing the difference between two classes two sampling- based approaches can be employed: under-sampling and over-sampling. The under-sampling method is used to decrease the dataset size by removing instances from the majority class that are selected at random. Less accuracy could occur as a result of the accidental deletion of crucial data. Examples in the minority class are randomly duplicated using the over-sampling technique. This method avoids losing data, but it could be over fitted if there is a lot of duplicate data. SMOTE is employed in this paper to circumvent the issue of over fitting [10].

Result

The CIC-ToN-IoT dataset, developed by the Canadian Institute for Cyber security (CIC) in 2019, is designed to evaluate IDS in IoT

environments. It captures realistic network traffic from IoT devices and traditional systems, simulating real-world traffic behaviours and attack scenarios. The dataset contains over 20 million records, offering a modern and challenging environment for intrusion detection research. The dataset includes 44 features, covering flow-based, content-based, and time-based attributes. It is labeled to indicate whether the traffic is benign or malicious, with the malicious traffic categorized into seven types of attacks: Backdoor, Denial of Service (DoS), DDoS, Infiltration, Injection, Man-in-the-Middle (MITM), and Ransom ware. The dataset is split into training and testing subsets, making it suitable for evaluating machine learning and deep learning models for IDS.

LIME has been particularly effective in NIDS by providing feature importance for individual instances, helping to identify the temporal and spatial patterns crucial for detecting attacks like Distributed Denial of Service (DDoS) or zero- day exploits. In models handling both temporal and spatial data, such as Seq2Seq or Conv LSTM, LIME offers real- time interpretability, showing how specific features influence intrusion detection over time. This helps ensure that models learn relevant dependencies in the data, improving their effectiveness at identifying complex attack patterns [11]. Additionally, LIME enhances the accountability of NIDS models by allowing analysts to verify that the model's decisions are based on meaningful, security-relevant features rather than spurious correlations.

TABLE 2: Precision, Recall, F1-Score compared on UNSW-NB15 dataset.

Evaluation Metric	Seq2Seq	LuNET	**Hybrid Model**
Precision benign	0.98	1.00	**0.98**
Precision Attack	0.94	0.80	**0.95**
Recall benign		0.95	

	0.98		**0.98**
Recall Attack		1.00	
	0.94		**0.97**
F1-Score benign		0.97	
	0.98		**0.98**
F1-Score Attack		0.89	
	0.94		**0.96**

The proposed hybrid model integrates convolutional and recurrent neural network layers to process temporal and spatial features effectively. The encoder begins with an input layer accepting variable-length sequences, followed by a ConvLSTM1D layer with 128 filters and a kernel size of 4 to extract spatiotemporal patterns. This is followed by a MaxPooling2D layer to reduce the spatial dimensions, ensuring computational efficiency. Spatial features also play a significant role in attack detection. For example, the Dest Port value of −0.28 suggests targeted traffic directed at specific ports, a characteristic often found in targeted attacks where specific vulnerabilities are exploited [12]. The Init_Win_bytes_forward value of 0.91 shows a minimal initial window size in the forward direction, a tactic frequently used in attacks to disrupt normal connection establishment and target system resources. Together, these temporal and spatial features highlight significant abnormalities in the traffic flow, packet size, and communication direction.

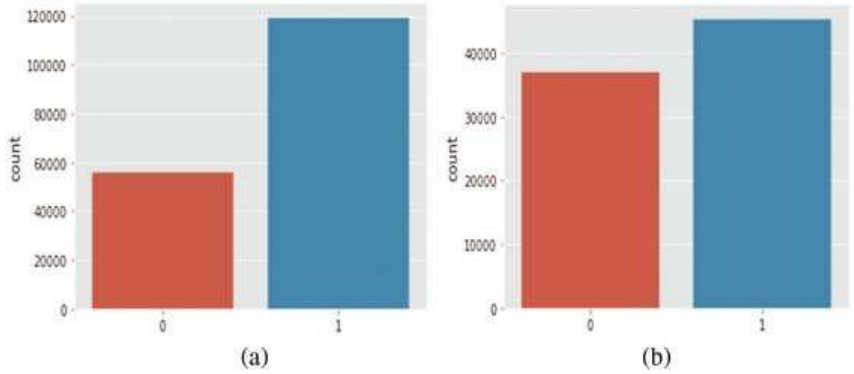

Figure 3: Data distribution (a) before SMOTE (b) after SMOTE in UNSW-NB

By fine-tuning these extra hyper parameters, the hybrid model performs better. The performance of the hybrid model can be significantly increased by determining the appropriate amount of hyper parameters and fine-tuning them. These hyper parameters improve the effectiveness of feature selection and subsequently classification by preventing over fitting and under fitting and also reduce the computation cost by selecting only important features [13]. To perform binary classification, the datasets were split into two groups: benign and assault.

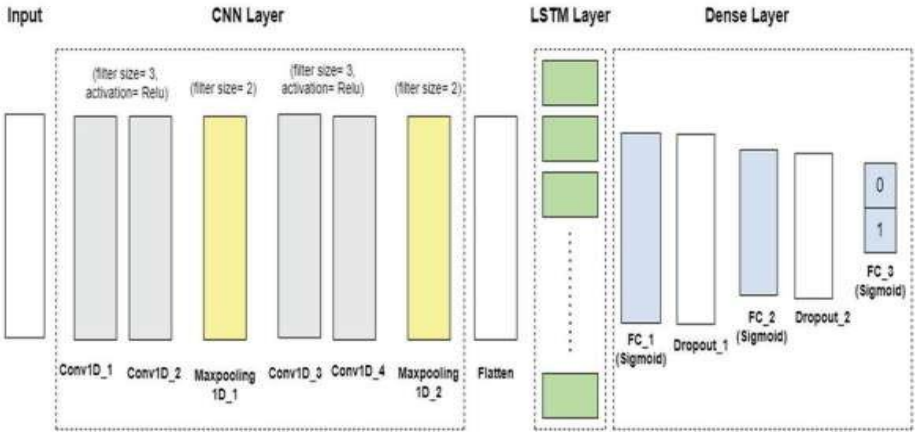

Figure 4: Proposed model architecture

when conducting the trials. The results for the RNN approach achieved an accuracy of 87.21%, an F1 score of 94.03%, and a validation accuracy of 95.93%. 180 RNN units were utilized in the hidden layers of this classifier, and it took 139.55 seconds to train [14]. A model with 180 LSTM units spread over 5 layers achieved a test accuracy of 88.41%, an F1 score of 98.64%, and a validation accuracy of 98.25% when it came to the LSTM approach. The best classifier in the GRU algorithm example achieved an88.55% test accuracy, a 95.61% F1 score, and a 152.17-second training time by using the NSL-KDD dataset's reduced feature vector, we ran simulations on it during the second stage of our experiment. We took into consideration the LSTM, GRU, and RNN algorithms. The outcomes for the binary classification scheme are. RNN's dense layer's Re LU activation function yielded a training time of 85.32%, an F1 score of 89.48%, and an88.71% test accuracy. The results show that the most effective model, the RNN, obtained a test accuracy of 83.20%, an F1 score of 87.09%, and a validation accuracy of 88.77%. With 180 units in the hidden layers, this classifier yielded a training time of 158.65 seconds. The most effective model was trained in 195.85 seconds with 180 units in the hidden layers, and it achieved a test accuracy of 97.91% and a validation accuracy of 98.25%. The results provided by the best RNN model are not as good as those achieved by the LSTM in terms of test accuracy [15]. the training time-frames of each model on the NSL KDD and UNSW NB15 datasets respectively for the LSTM multiclass classification job. The trends show that the LSTM has the longest training period for a sophisticated RNN. In a subsequent stage, we selected two datasets- CIC IDS 2017 and WSN DS-to apply the CNN-LSTM model.

Table 3: Performance evaluation of LSTM model and Hybrid LSTM-GRU and 1D CNN model

Model	**Accuracy**	**Val Acc**	**Loss**	**Val Loss**
LSTM Model	0.99	0.98	0.01	0.55
Hybrid LSTM- GRU and 1D CNN model	0.99	0.97	0.01	0.07

Machine Learning and Deep Learning Modeling

Create a hybrid neural network that is based on LSTM and 1D-CNN. In addition to this, implement state-of-the-art machine learning algorithms such as the random forest, decision tree, support vector machine, naive Bayes, and logistic regression.

Performance Evaluation

Following training, the performance of the models will be evaluated using matrices such as accuracy, precision, recall, f-score, and loss of models. We overcame this obstacle by comparing the outcomes of an empirical experiment we ran on well- known CNN-based methods using industry-standard datasets. The suggested model's LSTM, Hybrid LSTM-GRU, & 1D CNN models' performance evaluations are presented. One popular statistic for evaluating performance is accuracy, which is defined as the percentage of correct classifications relative to the total. One should not rely on accuracy as a measuring tool in the presence of an imbalanced dataset.

Conclusion

The investigation of ML/DL hybrid models for social media attack prediction and detection demonstrates that combining machine learning's feature extraction capabilities with deep learning's ability to capture complex temporal and spatial patterns significantly enhances detection performance. Hybrid models effectively address challenges such as high-dimensional data, imbalanced attack distributions, and the dynamic nature of social media environments. The research highlights that architectures integrating CNNs, LSTMs, GRUs, and autoencoders provide robust, adaptive, and real-time solutions for identifying malicious activities. Overall, ML/DL hybrid frameworks represent a promising approach to strengthening social media cyber security, enabling proactive attack prediction and mitigation while ensuring safer and more reliable online communication platforms.

Reference

1. Akhtar, M. S., & Feng, T. (2022). Detection of Malware by Deep Learning as CNN-LSTM Machine Learning Techniques in Real Time. Symmetry, 14(11), 2308.

2. Liu, Y., Wang, X. K., Hou, W. H., Liu, H., & Wang, J. Q. (2022). A novel hybrid model combining a fuzzy inference system and a deep learning method for short-term traffic flow prediction. Knowledge-Based Systems, 255, 109760.
3. Mahajan, S., HariKrishnan, R., & Kotecha, K. (2022). Prediction of network traffic in wireless mesh networks using hybrid deep learning model. IEEE Access, 10, 7003-7015.
4. Petmezas, G., Haris, K., Stefanopoulos, L., Kilintzis, V., Tzavelis, A., Rogers, J. A., ... & Maglaveras, N. (2021). Automated atrial fibrillation detection using a hybrid CNN-LSTM network on imbalanced ECG datasets. Biomedical Signal Processing and Control, 63, 102194.
5. Rizvi, S., Scanlon, M., McGibney, J., & Sheppard, J. (2022). Deep learning based network intrusion detection system for resource-constrained environments. In Springer (pp. 1-7).
6. Sasidhar, T. T., Premjith, B., & Soman, K. P. (2020). Emotion detection in hinglish (hindi+ english) codemixed social media text. Procedia Computer Science, 171, 1346-1352.
7. Satyanegara, H. H., & Ramli, K. (2022). Implementation of CNN-MLP and CNN-LSTM for MitM Attack Detection System. Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 6(3), 387-396.
8. Song, Z. English speech recognition based on deep learning with multiple features. Computing 2020, 102, 663–682.
9. Tian, C.; Fei, L.; Zheng, W.; Xu, Y.; Zuo, W.; Lin, C.-W. Deep learning on image denoising: An overview. Neural Netw. 2020, 131, 251–275.
10. J. Hussain and V. Hnamte, ‘‘Deep learning based intrusion detection system: Modern approach,’’ in Proc. 2nd Global Conf. Advancement Technol. (GCAT), Oct. 2021, pp. 1–6
11. A. H. Nasreen Fathima and S. P. S. Ibrahim, ‘‘Multi-stage deep investigation pipeline on detecting malign network traffic,’’ Mater. Today, Proc., vol. 62, pp. 4726–4731, Jan. 2022,
12. Y. A. Jerusha, S. P. S. Ibrahim, and V. Varadharajan, ‘‘An effective network intrusion detection model

for coarse-to-fine attack classification of imbalanced network traffic,'' Int. Res. J. Adv. Sci. Hub, vol. 5, pp. 531–540, May 2023.

13. W. Khan, M. Haroon, A. N. Khan, M. K. Hasan, A. Khan, U. A. Mokhtar, and S. Islam, ''DVAEGMM: Dual variational autoencoder with Gaussian mixture model for anomaly detection on attributed networks,'' IEEE Access, vol. 10, pp. 91160–91176, 2022.
14. S. M. Kasongo and Y. Sun, ''A deep gated recurrent unit based model for wireless intrusion detection system,'' ICT Exp., vol. 7, no. 1, pp. 81–87, Mar. 2021.
15. V. Hnamte and J. Hussain, ''DCNNBiLSTM: An efficient hybrid deep learning-based intrusion detection system,'' Telematics Informat. Rep., vol. 10, Jun. 2023, Art. no. 10005.