International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Intrusion Detection and Irregularity Analysis in 5g Networks using Deep Learning

Nisha

Research Scholar, Department of Computer Science and Applications, Baba Mastnath University, Rohtak, Haryana, India

ABSTRACT- The proliferation of Internet of Things, or IoT, equipment and the introduction of 5G networks have resulted in an explosion of data that is both copious and highly interconnected. There is an immediate need for strong Intrusion Detection Systems (IDS) designed for IoT ecosystems since this highly linked environment poses serious security risks. In this research, we look at how 5G-enabled IoT environments might benefit from deep learning architectures for intrusion detection system development. It assesses the efficacy of four state-of-the-art models in particular: CNN-BiGRU, TCN + LSTM, CNN-Bidirectional LSTM with Attention and Hierarchical Recurrent Neuronal Networks (HRNN). To find out how well each model can spot irregularities and possible security breaches, we run a thorough comparison study, paying special attention to important performance measures like loss and accuracy. Training performance is best for the TCN + LSTM architecture (with a loss of only 0.03 out of all the models tested), while CNN-BiLSTM + Attention comes in second with 94.2% accuracy & a loss of only 0.06. These results greatly aid in the creation of smart, IDS frameworks powered by deep learning, which improve the robustness and safety of IoT networks in the age of 5G connectivity. Furthermore, the findings provide important information regarding the practical use of these mathematical models for protecting smart environments in the future.

Keywords: *Deep Learning, Intrusion Detection, Internet of Things, 5G Networks, HRNN, CNN-BiGRU, TCN, BiLSTM, Attention Mechanism)*

I. INTRODUCTION

The IoT, or the Internet of Things has become a pervasive presence in today's hyperconnected society, allowing physical things and gadgets to be effortlessly integrated into the digital sphere. A new era of efficiency and convenience has been brought about by the Internet of Things' rapid growth throughout industries, including smart homes, transportation, healthcare and agriculture. But as IoT devices proliferate at an exponential rate, worries about security and privacy have also escalated to previously unheard-of heights. A major difficulty in an IoT ecosystem is making sure that infrastructure, networks and sensitive data are protected[1]. Here, new possibilities and threats have emerged as a result of the confluence of the Internet of Things (IoT) with the low-latency, high-speed capabilities of 5G networks. The development of advanced intrusion detection technologies (IDS) has grown in importance for the purpose of fixing potential security vulnerabilities. This introductory section gives a synopsis of the development of the Internet of Things, the launch of the 5G networks and the pivotal function of deep learning. plays in developing an effective intrusion detection system for this environment[2].

A. THE RISE OF IOT

In the early 2000s, the first signs of what would later be known as the Internet of Things emerged: a network of networked devices. The widespread practice of linking commonplace items, machines and technologies to the internet to enable data gathering and communication is known as the "Internet of Things" (IoT). Smart homes automate mundane tasks, while industrial IoT enhances supply chain oversight and manufacturing processes; these are just a few of the many benefits that have arisen as a consequence of this interconnectedness.[3]. As the number of Internet of Things (IoT) devices has grown over the last decade, the potential for innovative uses has seemed limitless. However, a shadowy aspect of the Internet of Things became apparent with its rapid expansion. With more connections, bad actors have a bigger target to attack. Due to a lack of adequate security measures, IoT devices are vulnerable to various cyber threats. Due to the rise in intrusions, data breaches and assaults on critical infrastructure, the Internet of Things (IoT) ecosystem requires robust security solutions.[4].

B. THE NEED FOR INTRUSION DETECTION SYSTEMS

An integral part of any thorough cybersecurity plan should include intrusion detection systems, which keep an eye on network traffic, look for unusual patterns and either notify the proper people or take action in response to emerging dangers. It is much easier to see why IDS is necessary when 5G and the Internet of Things are considered. Given the rapid pace of change and the linked nature of our society, it is possible that some threats may evade traditional intrusion detection systems. 5G networks and IoT devices pose specific dangers due to their design and operation. IoT devices often have low computing power, making them susceptible to resource-intensive attacks. Furthermore, because IoT devices are used in a variety of challenging locations, they are more vulnerable to physical manipulation and assaults. With regard to 5G, the widespread application of edge computing and network slicing creates a complex network topology that calls for sophisticated and flexible intrusion detection[5]-[6].

C. DEEP LEARNING'S ROLE

The ever-changing and interdependent Internet of Things (IoT) in the context of 5G has opened up new possibilities in technology, but it has also brought up major worries about safety. As the nature of threats evolves, deep learning—a state-of-the-art branch of machine learning—has shown encouraging results. Regarding 5G networks, computational models, especially neural networks, have demonstrated significant potential for transforming the security of the Internet of Things. Their innate ability to autonomously analyse complex databases, allowing them to detect minute patterns and irregularities, is the main cause for this change. To better understand how intrusion detection systems that rely on deep learning can keep 5G-enabled Internet of Things (IoT) networks and devices safe, this study delves into their theoretical foundations. Finding connections in highly dimensional information, which is common in 5G network IoT situations, can be challenging. Many have lauded deep learning models for their capacity to do this. Due to their reliance on static signatures and criteria, classic intrusion detection methods could not keep up with the dynamic nature of online hazards. However, deep learning offers some adaptability since it can discover novel attack paths automatically.[7]–[9].

D. DEEP LEARNING: THE BEST OPTION FOR 5G IOT

As the Internet of Things (IoT) evolves within 5G networks, deep learning will become increasingly important as a security measure. It is the greatest choice for lowering security worries due to its adaptability, scalability and ability to handle high-dimensional data. The safety of ecosystems based on and the efficient functioning of 5G networks are both aided by intrusion detection systems that use deep learning to swiftly identify and mitigate security threats. In keeping with the ever-changing nature of IoT security, this approach is well-suited to deal with the challenges posed by the merging of IoT and 5G technologies

Due to its independence in evaluating huge datasets, adeptness in detecting complex patterns and anomalies and adaptability to evolving security threats, deep learning is revolutionising security for the Internet of Things in 5G networks. Built on neural networks and taught on massive datasets, these state-of-the-art intrusion detection systems provide formidable resistance to the ever-evolving threat landscape. As the Internet of Things (IoT) and 5G networks expand, deep learning will play an increasingly important role in ensuring the safety of the digital societies of the future.[10].

E. NEURAL NETWORKS IN INTRUSION DETECTION

Deep learning intrusion detection systems rely on neural networks as their central technology. Interconnected layers of synthetic neurones make up artificial neural networks, which take their cues from the way the human brain processes information. Pattern recognition is one of their strong suits and they have proven adept at detecting sophisticated intrusion efforts.
The ability of intrusion detection systems powered by deep learning to detect anomalies in device behaviour and network traffic automatically is a major advantage of these systems. These out-of-the-ordinary occurrences may indicate malicious intent, unauthorised entry, or data breaches. Due to their reliance on manually created rules, conventional systems struggled to adapt to hackers' ever-changing techniques. In contrast, deep learning models excel at seeing subtle departures from established patterns, which gives them the ability to detect complex but before unseen dangers. One further thing that shows how great this technology is is deep learning's capacity to process and learn from massive datasets. In the context of intrusion detection, these datasets are crucial for training neural networks to differentiate between malicious and benign behaviour. With the right amount of training data, the models can pick up on subtleties in normal network traffic dynamics, patterns of communication and the way Internet of Things (IoT) devices behave. After receiving so extensive training, the models may detect irregularities that may indicate an intrusion or security breach. The complexity of modern assaults necessitates systems that are tailor-made to identify breaches using deep learning. As attacker complexity has grown, so has the inadequacy of traditional signature-based methods. Although they may not exhibit patterns or leave conventional evidence, deep learning methods can detect complex, multi-stage assaults. So, these technologies can improve the security of 5G networks' Internet of Things devices by detecting new and cryptic attack vectors.[11]–[14].

II. LITERATURE REVIEW

Mishra 2023 et. al Develop a prediction tool for network-wide detection that can discriminate between "appalling" associations—also known as incursions or assaults—and "high quality" or common connections. The objective was to assess the outcomes in terms of accessibility. Additionally, we focused on machine learning-based classification in our Knowledge Discovery Cups 1999 dataset for prediction to obtain optimal training and testing outcomes and to apply our approach for utilizing contemporary technologies. used a variety of machine learning-based techniques to generate several classification models, comparing them to determine which model best suits computer networks in terms of time and accuracy[15].

Lin 2022 et. al In terms of identifying network denial-of-service (DoS) attempts, packet flows are a good way to go (0.82), while the log data works best (0.94) during the initial attack stage. Additionally, when using all three data sources to complete this detection, there are minimal expenses of no more than 2.1% Central processing unit utilisation. Finally, investigators look at important parts of each model, such as the amount of logs generated by Apache-Access in the telnetd and postfix log datasets, SrcBytes or TotBytes, MINFLT, VSTEXT and RSIZE.[16].

Mandru 2022 et. al IDS (DNN) requires deep neural networks to be connected in order to function. DNNs should not anticipate assaults on the N-IDS throughout the course of this report. Our DNN for the 1000-the year assortment has an average growth rate of 0.1. In order to determine preparedness and site meaning association, the KDDCup-'99' informative index was employed. To make assessment easier, the setup is finished on a related dataset with an additional old AI figure and a DNN with levels ranging from 1 to 5. Following the breakdown of the results, it was determined that the optimal choice for implementation would be a DNN consisting of three tiers[17].

Yadav 2022 et. al It will be straightforward to identify actual worldwide intruders with the proposed intrusion detection architecture. One very effective usage of neural networks is attack detection. The importance of providing cybersecurity solutions with a focus on the end user is also growing. Because of this, 5G networks will need to collect, analyse and analyse massive amounts of data traffic and network connections. A comparison of the various models' detection times and precisions reveals that the automatic encoding model outperforms them all. The suggested method yielded a precision of 99.76 percent.[18].

Vaigandla 2022 et. al There are expanding problems and the way forward is not obvious. There are a growing number of challenges around the security of the Internet of Things. There are a lot of ones already out there, but there has to be a lot more for the security of IoT networks. Using machine learning is one way to make the Internet of Things more secure. In this research, we take a look at many deep learning and machine learning techniques, as well as common IoT protection data sets. Using deep learning, researchers have created an algorithm that can detect denial-of-service (DoS) attacks. This research makes use of Python programs and libraries like Tensorflow, Sea born and Scientist Learning. Researchers have found a deep learning model that might improve the accuracy of threat mitigation in an IoT network.[19].

Elghamrawy 2022 et. al We offer an intrusion detection model that makes use of deep learning. This model is based on a neural network called a multi-layer per (MLP). Using the KDDCUP 99 dataset, this study compared two deep learning algorithms both to one other and to previous studies. Both designs incorporate four hidden levels of ReLu activation, an Adam optimiser, an output that activates softmax and validation loss monitoring that ends early. Like other multi-classification neural networks, they use categories cross entropy to compute loss functions. Model 2's hidden layers were (10, 20, 20, 1) and Model 1's (10, 50, 10, 1), respectively. Model 2 architecture has a maximum accuracy of 99.785% and Model 1 architecture has a maximum precision of 99.88%. When assessing the system's accuracy and efficiency, the sample size was considered.[20].

Sirag 2022 et. al A plethora of research is underway to identify possible remedies for this issue. Anomaly detection is the crux of intrusion detection; it uses alerts from normal operations to reveal the existence of assaults (intentional or otherwise), errors, vulnerabilities and other issues. These papers provide a thorough literature overview of machine learning techniques for intrusion detection, with a focus on Random Forest or Support Vector Machine applications. Reading aloud and summarising each method according to its developing way relevance and reference number, articles give a detailed description of each approach.[21].

TABLE-1 LITERATURE SUMMARY

Author / Year	**Model**	**Results**	**Refrences**
Alfoudi/2022	DBSCAN , IDS	Acc=90.03 %	[22]
Banaamah/ 2022	denial-of-service (DoS)attacks, IoT,CNN, MLP	Acc=91.27 %	[23]
Yilmaz/ 2022	SVM,NN	Acc=77%	[24]
Fatani/ 2022	AQU,CNN, swarm intelligence (SI) algorithms	Acc=82.7%	[25]

Chindove/ 2021	NIDS model, RF,KNN,MLP	Acc=98.7%
		Precision=90 %
			[26]

Tang/2018	GRU-RNN, SDN	Acc=89%	[27]
Kim/2018	Deep Neural Networks, Neural Networks	Acc=96.7%	[28]

III. PROPOSED METHODOLOGY

The Cyber Range Lab at the School of New South Wales, Canberra, developed the UNSW-NB15 dataset and the first step is to import it using the IXIA PerfectStorm program. For the purpose of doing research on intrusion detection, this dataset simulates real-world network traffic and cyberattacks. We used Tcpdump to gather almost 100 GB of raw data in Pcap format. Shellcode, worms, analysis, backdoors, detectors and generic attacks are among the nine kinds of assaults included in the dataset. For enhanced comprehension and analysis, we have given feature definitions with the traffic statistics. You can see Exploratory Data Analysis (EDA) in action in Figure during the pretreatment step, which includes gathering the data, model cleaning, deployment and results evaluation. 1.

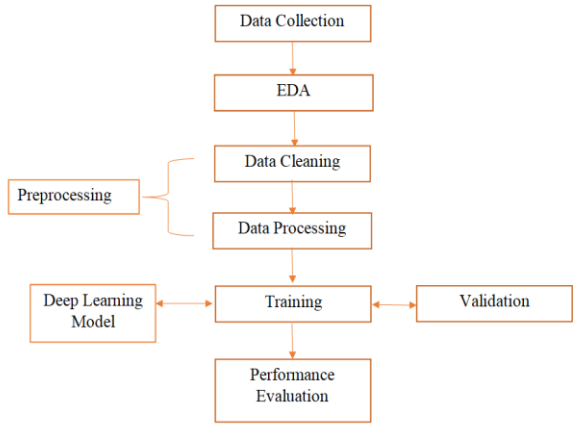

Fig. 1 Proposed Flowchart

A. Data Collection

This study relies on data obtained from the following source: https://www.kaggle.com/datasets/mrwellsdavid/unsw-nb15/code. The Cyber Range Lab at the Catholic University of New South Wales in Canberra, used the IXIA PerfectStorm program to simulate common network operations and simulated cyber-attack behaviours. They used these simulations to build the UNSW-NB15 dataset. The purpose of this endeavour was to deepen our comprehension of how cyber assaults affect network infrastructure. When we used Tcpdump to save the raw traffic data as Pcap files, we got almost 100 GB of it. There are a total of nine different kinds of attacks included in the dataset, including fuzzers, analysis, backdoors, DoS, exploits, generic assaults, shellcode, worms, or reconnaissance. Worms are one kind of replicating itself malicious software that falls within these classes, which include both simple and complicated forms of malevolent behaviour.

B. Data Pre-processing

In order to create intrusion detection systems that can effectively safeguard networks and systems from malware, hackers and other security threats, data preprocessing is an essential step. Data preparation is key to improving the system's anomaly detection accuracy. Eliminating superfluous or unneeded characteristics is a part of this process to make computations more efficient and less noisy. In order to avoid detecting false positives, outlier values are limited. Applying log transformations to skewed numerical data normalises it, allowing for the discovery of hidden patterns. Improving machine learning models' capacity to differentiate between typical and out-of-the-ordinary behaviour is possible via lowering skewness. Training time and model complexity can both rise in datasets that have many different labels for categorical characteristics. By applying label encoding or one-hot encoding to groups of comparable labels, we can simplify the data and increase the model's generalisability. When data is properly prepared, intrusion detection systems are better able to spot malicious activity, identify threats more quickly and make 5G and IoT networks more secure.

C. Exploratory Data Analysis (EDA)

To gain deeper insights into the differences between benign and malicious intrusions, conducting Exploratory Data Analysis (EDA) is essential. EDA involves applying techniques such as statistical summaries, visualizing feature distributions, identifying class imbalances, analyzing correlations and detecting anomalies. These methods help simplify high-dimensional data through time series analysis and dimensionality reduction, enabling better understanding and interpretation.

Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

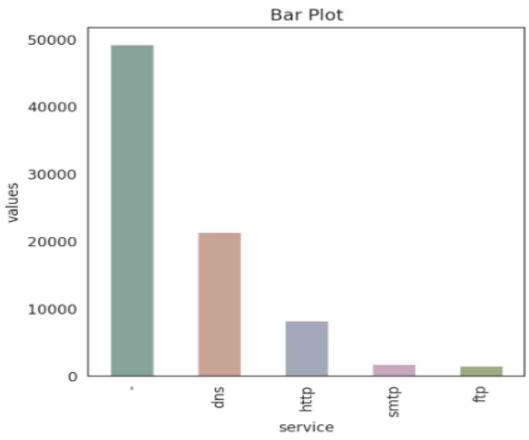

Fig. 2 bar plot of ser

Figure 2 illustrates a bar plot that displays the distribution of service attributes within the dataset. Each bar represents a unique service type, with its height corresponding to the frequency of occurrence. This visual representation provides a clear overview of how often each service appears, helping to highlight both common and rare attributes. Such insights are valuable for guiding data preparation and selecting effective models for intrusion detection.

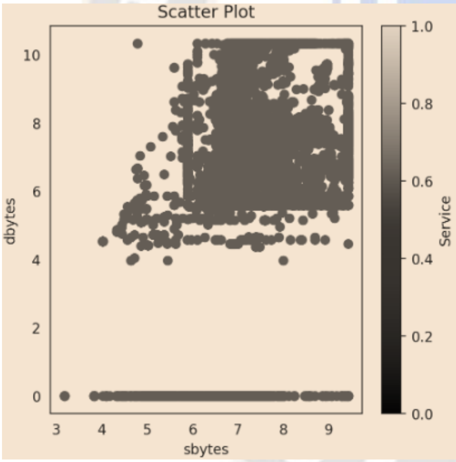

Fig. 3 Scatter plot of source bytes and destination bytes

Figure 3 presents a scatter plot, a two-dimensional graphical representation used to explore the connection between a pair of numerical parameters. Here, the x-axis shows the number of bytes that came from the source and the y-axis shows the number of bytes that went to the destination. This visual aid is useful for examining the distribution and potential correlation between these variables, providing insights into network traffic behavior that may indicate normal or anomalous activity.

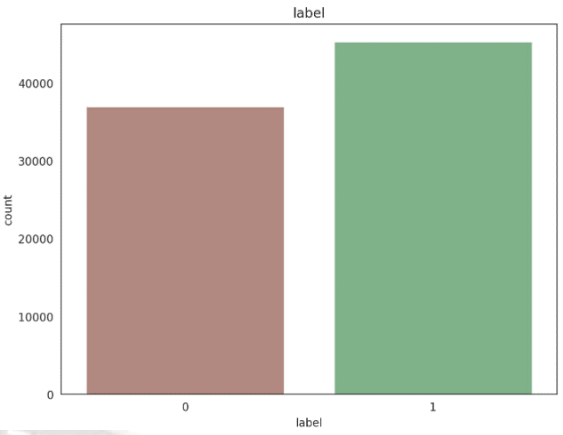

Fig. 4 Count plot of label attribute

Figure 4 provides a visual representation of the dataset's 'label' attribute distribution through a count plot. This plot shows the frequency of each distinct label category, providing a straightforward overview of how many instances belong to each class—such as benign or malicious—within the dataset.

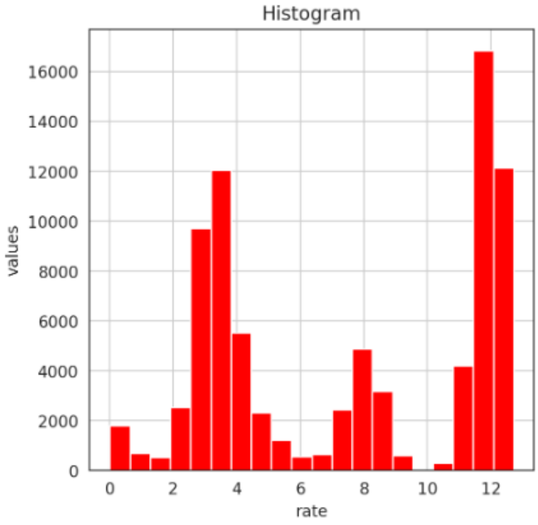

Fig. 5 Histogram of rate and values

Figure 5 presents a histogram that illustrates the distribution of the 'rate' attribute values in the dataset. The histogram groups these values into discrete intervals (bins), offering a clear visual representation of their frequency and overall distribution pattern.

D. Data Splitting

For testing and training reasons, it is common practice to divide a dataset into smaller subsets, a technique known as data splitting. In order to determine how well, how generalisable and how effective a model is in real-world situations, this phase is crucial. To guarantee accurate model validation, this study divided the dataset in half: 80% for use in training and 20% for testing.

***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

E. Deep learning Modelling

A number of state-of-the-art deep learning architectures have shown promising results for intrusion detection tasks. These include CNNs combined with Bidirectional gates of recurrent units (CNN-BiGRU), TCNs integrated with long- and short-term memory networks (TCN + LSTM) and Hierarchical Recurrent Neural Networks (HRNNs). When applied to time-series data, such as that found in system logs and network traffic, these models shine. In complicated Internet of Things (IoT) or multi-layer network situations, HRNNs shine at capturing hierarchical timing structures, which allows the algorithm to learn patterns across several levels of abstraction. Improving the detection of both emerging and current threats, CNN-BiGRU models efficiently extract local patterns using convolutional layers as capture bidirectional temporal connections using GRUs. Combining TCNs' efficient long-range temporal modelling with LSTMs' memory capabilities, the TCN + LSTM architecture provides improved accuracy in detecting delayed or subtle abnormalities. Organisations can improve their detection accuracy, generalisation to undiscovered attack patterns and adaptive response to future cybersecurity threats by utilising these strong models in the construction of intrusion detection systems.

- **HRNN**

The purpose of Hierarchical Recurrent Neural Networks is to detect hierarchical degrees of structured correlations in sequential data. Human recurrent neural networks (HRNNs) differ from regular RNNs in that they sort input into levels (such as characters → words → words or packets → sessions → traffic flows) and employ a distinct recurrent unit to handle each level. This is why HRNNs are perfect for complicated IoT security jobs, as network traffic can show patterns throughout time and throughout protocol layers. They are able to better describe long-range dependencies and provide superior abstractions because to their layered architecture.

- **CNN-BiGRU**

Here, the best features of both CNNs and Bidirectionally Gated Recurrent Units (BiGRUs) come together in a hybrid design. Network traffic often exhibits periodic patterns, signal peaks, or traffic bursts and the CNN layers serve as effective feature extractors by detecting these patterns. Layers within the BiGRU architecture process the data in both the forward or backward temporal directions after receiving the extracted features. Because it can take in information from both the past and the future, this model is great for finding intrusions and anomalies that depend on one another in a sequential fashion.

- **TCN + LSTM**

The model takes advantage of the ways in which LSTM and Temporal Convolutional Networks (TCNs) interact together. TCNs provide stable gradients across lengthy sequences and speedier training by efficiently modelling long-range temporal dependencies using dilated causal convolutions. On the other hand, LSTMs' gating mechanisms give memory, whereas TCNs do not. The design takes advantage of TCNs' efficient temporal modelling and incorporates an LSTM layer after them to keep track of previous states in long-term memory. For continuous IoT traffic streams, this combination is ideal for detecting delayed or subtle intrusions.

- **CNN-BiLSTM + Attention**

For intrusion detection in complicated network settings, the CNN-Bidirectional LSTM with Care (CNN-BiLSTM + Attention) model is an excellent choice due to its strong deep learning architecture's ability to efficiently grasp patterns of time and space in sequential data. To start, this hybrid model uses one-dimensional convolutional layers to pull out specific information from unprocessed sequences of data, like logs or network traffic. These convolutional neural network (CNN) layers excel in spotting localised, short-lived anomalies, which are frequently signs of bad actors. Following feature extraction, the data is fed into Bidirectional short- and long-term memory (BiLSTM) layers for both backward and forward temporal processing. The model can learn more about the sequence as a whole thanks to its bidirectional structure, which lets it remember information from both previous and subsequent time steps. To make the model even more task-specific, it incorporates an attention mechanism that dynamically gives more or less weight to individual time steps depending on how important they are. To improve detection accuracy and interpretability, this method makes sure the model focusses on the most informative bits of the input. In sum, the CNN-BiLSTM with Pay attention architecture is an effective method for detecting numerous intrusions in 5G-enabled and Internet of Things (IoT) network settings because it integrates the advantages of adaptive focus, spatial feature extraction and temporal context modelling.

IV. RESULT & DISCUSSION

Machine learning algorithms can have their efficacy in dealing with novel, unknown data measured quantitatively. To find out how useful a model is in the real world, this assessment is crucial. In this context, you might hear a few basic ideas like

1) TN/TP/FN/FP:

True Positive (TP): When the result is comparable to what was anticipated..

False Positive (FP): Despite the seemingly hopeful nature of the results, were actually depressing.

True Negative (TN): when something that was expected to go wrong actually does go wrong.

False Negative (FN): The findings exceeded even the most modest of expectations, which were not particularly high.

2) Confusion Matrix:

Processing, cleaning and preparing the data are the stages before feeding it into an exceptional model that yields probabilistic conclusions. Oh, come on! How precisely can we tell if the model is working? are trying to improve our efficiency and output by deciphering the significance of the Confusion Matrix. This matrix is a crucial performance metric for classification jobs in machine learning.

3) Accuracy

A popular way to express accuracy is as an amount of the total data instances. Accuracy can be defined as "the amount of the total dataset examples that fit the right categorisation.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

4) Loss

Might incur some financial loss if that forecast proves to be incorrect. A "loss" is the numerical representation of the model's failure to correctly forecast an event's outcome under certain supplementary conditions. As a direct consequence, losses will be far higher if a model's prediction turns out to be wrong than if the prediction had been correct. In order to find out if the biases and weights are distributed fairly, models must go through training.

$$Loss = -\frac{1}{m}\sum_{i=1}^{m} \quad Yi.\log(Yi)$$

(2)

TABLE 2 HYPERPARAMETER DETAILS

Model	**HRNN, CNN-BiGRU, TCN + LSTM, CNN-BiLSTM with Attention**
Activation	Relu
Epochs	10
Batch size	2000
Metrics	Accuracy, Loss
Input	56,1
Total Parameters	25751
Trainable Parameters	25751

Table 2 this study's models—the CNN-Bidirectional LSTM with Paying attention (CNN-BiLSTM + Attention), the Hierarchical Neural Networks (HRNN), the CNN-BiGRU and the TCN + LSTM—present a summary of the hyperparameter settings of these models. While training, each model used the function to activate ReLU for ten iterations with a batch size of two thousand. Two measures that show how well the models do in training and making predictions are accuracy and loss. There are a grand total of 25,751 parameter trains generated by the 56 features and 1 time step that make up the input data. Having trainable parameters makes the models more adaptable and successful in identifying intrusions in 5G and IoT network scenarios.

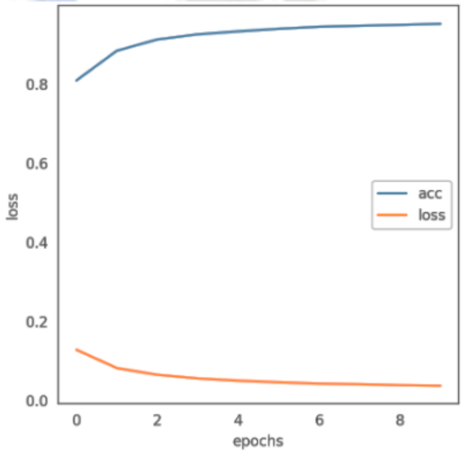

Fig. 6 Accuracy loss graph of hybrid HRNN

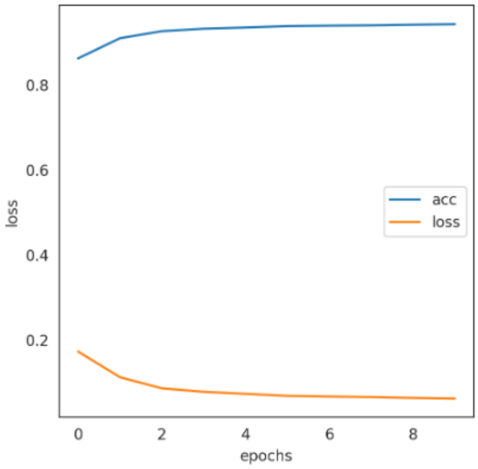

Fig. 7 Accuracy Loss graph of CNN-BiLSTM with Attention

TABLE 3 PERFORMANCE EVALUATION OF MACHINE LEARNING AND DEEP LEARNING MODELS

Model	Accuracy	Loss
HRNN	93.4%	0.16
CNN-BiGRU, TCN	93.8%	0.16
TCN + LSTM	95.1%	0.03
CNN-BiLSTM with Attention	94.2%	0.06

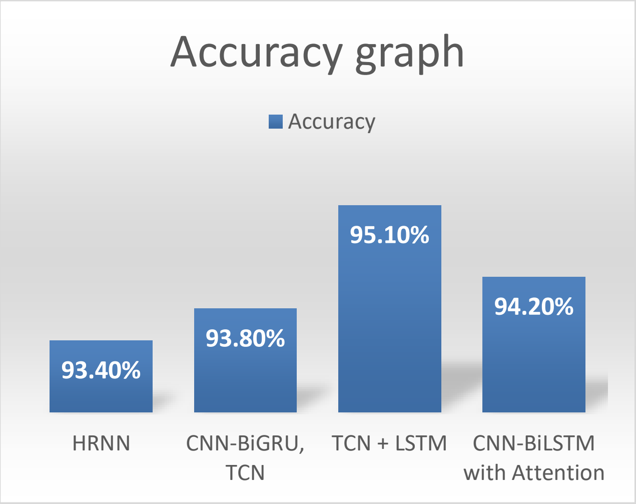

Fig. 8 Accuracy graph

This table compares and contrasts 5G and IoT intrusion detection methods that use deep learning. Metrics for accuracy and loss are the main points of comparison among the four models. We assess Hierarchical Recurrent Neural Networks (HRNN), Convolutional Neural Networks (CNN) with Bidirectional GRU (CNN-BiGRU), Convolutional Neural Networks (TCN) with Long Short-Term Memory (LSTM) and Cn-Bidirectional LSTM with Emphasis (CNN-BiLSTM + Attention). With a remarkable accuracy of 95.1% and the lowest loss value of 0.03 during training, the TCN + LSTM model proved to be the most promising method for intrusion detection. With a loss of 0.16 and an accuracy of 93.8%, the CNN-BiGRU model demonstrated strong performance, demonstrating its dependable detection capabilities. With a somewhat larger loss value of0.16, the HRNN model may have trained more efficiently, but it still attained an accuracy of 93.4%, which is equivalent. The CNN-BiLSTM using Attention model achieved 94.2% accuracy and kept its loss to 0.06 thanks to its attention mechanisms, bidirectional temporal modelling and effective spatial feature extraction. Its intrusion detection performance was high. With 5G and the Internet of Things posing their own set of security concerns, our findings shed light on how to choose the best deep learning approach for adaptive and resilient intrusion detection.

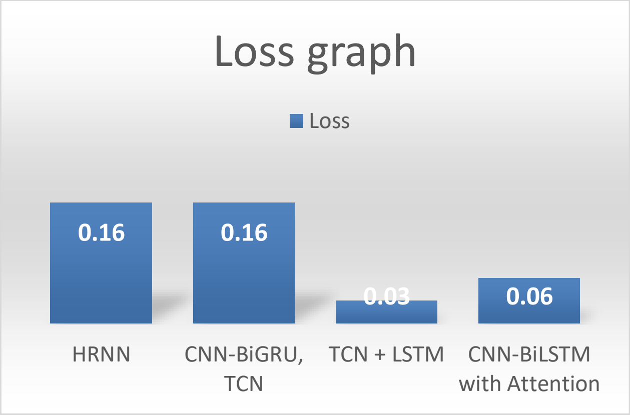

Fig. 9 Loss graph

V. CONCLUSION

To safeguard today's digitally interconnected world, it is crucial to implement a system to detect intrusions (IDS) within the context of the Internet of Things (IoT) enabled by 5G networks. To tackle the difficulty of detecting and mitigating security risks in such dynamic situations, this study assesses four sophisticated deep learning models: LSTM, GRU, Hybrid LSTM-GRU and CB-GRU. Because of their capacity to adapt to temporal fluctuations and catch sequential patterns, recurrent neural networks like LSTM and GRU are very good at anomaly detection. Combining the best features of both architectures, the Hybrid LSTM-GRU model achieves a better balance between memory retention and computational efficiency. It also shows better performance when it comes to modelling long-term dependencies, which are crucial for intrusion detection. The CB-GRU model combines the feature extraction capabilities of 1D CNNs with the temporal dependency capturing capabilities of Bidirectional GRUs. In intrusion circumstances, when sequential data is complex, this hybrid approach captures both local and global context, making it effective at handling the data. Based on the results of the comparison, the Hybrid LSTM-GRU model is the best one; it has excellent predictive power and training efficiency, with an accuracy of 95.1% and a loss of only 0.03. With a 0.16 loss and 93.8% accuracy, the GRU model was also dependable; LSTM, on the other hand, showed slightly lower training efficiency but still managed 93.4% accuracy. The CB-GRU model was a strong contender for real-world implementation due to its balanced performance, which it achieved with 94.2% accuracy and a loss of 0.06. Taken together, the results show that deep learning models and hybrid architectures in particular, have a lot of promise for protecting IoT-5G networks. This study confirms that hybrid techniques provide a strong combination of accuracy, adaptability and efficiency, but ultimately, the choice of model should be based on individual security requirements and system restrictions.

REFERENCES

[1] T. Su, H. Sun, J. Zhu, S. Wang and Y. Li, “BAT: Deep Learning Methods on Network Intrusion Detection Using NSL-KDD Dataset,” *IEEE Access*, vol. 8, pp. 29575–29585, 2020, doi: 10.1109/ACCESS.2020.2972627.

[2] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider and A. Wahab, “A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions,” *Electron.*, vol. 9, no. 7, 2020, doi: 10.3390/electronics9071177.

[3] A. Amouri, V. T. Alaparthy and S. D. Morgera, “A machine learning based intrusion detection system for mobile internet of things,” *Sensors (Switzerland)*, vol. 20, no. 2, 2020, doi: 10.3390/s20020461.

[4] Z. Wu, J. Wang, L. Hu, Z. Zhang and H. Wu, “A network intrusion detection method based on semantic Re-encoding and deep learning,” *J. Netw. Comput. Appl.*, vol. 164, no. March, 2020, doi: 10.1016/j.jnca.2020.102688.

[5] N. Satheesh *et al.*, “Flow-based anomaly intrusion detection using machine learning model with software defined networking for OpenFlow network,” *Microprocess. Microsyst.*, vol. 79, p. 103285, 2020, doi: 10.1016/j.micpro.2020.103285.

[6] P. Sun *et al.*, “DL-IDS: Extracting features using CNN-LSTM hybrid network for intrusion detection system,” *Secur. Commun. Networks*, vol. 2020, 2020, doi: 10.1155/2020/8890306.

[7] A. Derhab, “A Novel Two-Stage Deep Learning Model for Efficient Network Intrusion Detection,” vol. 7, 2019.

[8] T. T. H. Le, Y. Kim and H. Kim, “Network intrusion detection based on novel feature selection model and various recurrent neural networks,” *Appl. Sci.*, vol. 9, no. 7, 2019, doi: 10.3390/app9071392.

[9] H. Liu and B. Lang, “Machine learning and deep learning methods for intrusion detection systems: A survey,” *Appl. Sci.*, vol. 9, no. 20, 2019, doi: 10.3390/app9204396.

[10] H. Yao, D. Fu, P. Zhang, M. Li and Y. Liu, “MSML: A novel multilevel semi-supervised machine learning framework for intrusion detection system,” *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1949–1959, 2019, doi: 10.1109/JIOT.2018.2873125.

[11] M. A. Albahar, “Recurrent Neural Network Model Based on a New Regularization Technique for Real-Time Intrusion Detection in SDN Environments,” *Secur. Commun. Networks*, vol. 2019, no. Dl, 2019, doi: 10.1155/2019/8939041.

[12] C. Xu, J. Shen, X. Du and F. Zhang, “An Intrusion Detection System Using a Deep Neural Network with Gated Recurrent Units,” *IEEE Access*, vol. 6, pp. 48697–48707, 2018, doi: 10.1109/ACCESS.2018.2867564.

[13] D. Preuveneers, V. Rimmer, I. Tsingenopoulos, J. Spooren, W. Joosen and E. Ilie-Zudor, “Chained anomaly detection models for federated learning: An intrusion detection case study,” *Appl. Sci.*, vol. 8, no. 12, pp. 1–21, 2018, doi: 10.3390/app8122663.

[14] M. Zaman and C. H. Lung, “Evaluation of machine learning techniques for network intrusion detection,” *IEEE/IFIP Netw. Oper. Manag. Symp. Cogn. Manag. a Cyber World, NOMS 2018*, pp. 1–5, 2018, doi: 10.1109/NOMS.2018.8406212.

[15] N. Mishra and S. Mishra, “A Novel Intrusion Detection Techniques of the Computer Networks Using Machine Learning,” *Int. J. Intell. Syst. Appl. Eng.*, vol. 11, no. 5s, pp. 247–260, 2023.

[16] Y. D. Lin, Z. Y. Wang, P. C. Lin, V. L. Nguyen, R. H. Hwang and Y. C. Lai, “Multi-datasource machine learning in intrusion detection: Packet flows, system logs and host statistics,” *J. Inf. Secur. Appl.*, vol. 68, no. July, p. 103248, 2022, doi: 10.1016/j.jisa.2022.103248.

[17] D. B. Mandru, M. Aruna Safali, N. Raghavendra Sai and G. Sai Chaitanya Kumar, “Assessing Deep Neural Network and Shallow for Network Intrusion Detection Systems in Cyber Security,” *Lect. Notes Data Eng. Commun. Technol.*, vol. 75, no. May, pp. 703–713, 2022, doi: 10.1007/978-981-16-3728-5_52.

[18] N. Yadav, S. Pande, A. Khamparia and D. Gupta, “Intrusion Detection System on IoT with 5G Network Using Deep Learning,” *Wirel. Commun. Mob. Comput.*, vol. 2022, 2022, doi: 10.1155/2022/9304689.

[19] K. K. Vaigandla and R. Karne, “APPLICATIONS OF IOT ON INTRUSION DETECTION SYSTEM WITH

DEEP To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code," no. August, 2022, doi: 10.48047/IJIEMR/V11/SPL.

[20] S. M. Elghamrawy, M. O. Lotfy and Y. H. Elawady, "An Intrusion Detection Model Based on Deep Learning and Multi-layer Perceptron in the Internet of Things (IoT) Network," *Lect. Notes Data Eng. Commun. Technol.*, vol. 113, no. July, pp. 34–46, 2022, doi: 10.1007/978-3-031-03918-8_4.

[21] H. Sirag and S. D. Awadelkariem, "A Review on Intrusion Detection System Using a Machine Learning Algorithms," *Lect. Notes Networks Syst.*, vol. 322, pp. 281–290, 2022, doi: 10.1007/978-3-030-85990-9_24.

[22] A. S. Alfoudi *et al.*, "Hyper clustering model for dynamic network intrusion detection," *IET Commun.*, no. August, pp. 1–13, 2022, doi: 10.1049/cmu2.12523.

[23] / A. M. and I. Ahmad, "Intrusion Detection in IoT Using Deep Learning," *Sensors*, vol. 22, no. 21, 2022, doi: 10.3390/s22218417.

[24] A. A. Yilmaz, "Intrusion Detection in Computer Networks using Optimized Machine Learning Algorithms," *3rd Int. Informatics Softw. Eng. Conf. IISEC 2022*, no. October, 2022, doi: 10.1109/IISEC56263.2022.9998258.

[25] A. Fatani, A. Dahou, M. A. A. Al-Qaness, S. Lu and M. A. Elaziz, "Advanced feature extraction and selection approach using deep learning and aquila optimizer for iot intrusion detection system," *Sensors*, vol. 22, no. 1, 2022, doi: 10.3390/s22010140.

[26] H. Chindove and D. Brown, "Adaptive Machine Learning Based Network Intrusion Detection," pp. 1–6, 2021, doi: 10.1145/3487923.3487938.

[27] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi and M. Ghogho, "Deep Recurrent Neural Network for Intrusion Detection in SDN-based Networks," *2018 4th IEEE Conf. Netw. Softwarization Work. NetSoft 2018*, pp. 462–469, 2018, doi: 10.1109/NETSOFT.2018.8460090.

[28] D. E. Kim and M. Gofman, "Comparison of shallow and deep neural networks for network intrusion detection," *2018 IEEE 8th Annu. Comput. Commun. Work. Conf. CCWC 2018*, vol. 2018-Janua, no. October, pp. 204–208, 2018, doi: 10.1109/CCWC.2018.8301755.