IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 1, February 2025

Strengthening Cloud Cybersecurity with RNN Intelligence for Superior Intrusion Detection

Venkataramesh Induru[1], Priyadarshini Radhakrishnan[2], Yashwant Kumar Kolli[3]
Vijai Anand Ramar[4], Karthik Kushala[5], Thanjaivadivel M[6]
Piorion Solutions Inc, New York, USA[1]
Cognizant Technology Solutions US Corp, College Station, Texas, USA[2]
IBM Corporation, Ohio, USA[3]
Delta Dental Insurance Company, Georgia, USA[4]
Taylor Corporation, Minnesota, USA[5]
Nandha Engineering College, Erode, Tamil Nadu, India[6]
venkatarameshinduru@gmail.com, priyadarshinir990@gmail.com, yashkolli04@gmail.com
vijaianandramar@gmail.com, karthik.kushala@gmail.com, thanjaivadivelm@gmail.com

Abstract: *Needing protection became the security of digital infrastructure providers, thus even needing centralization of network intrusion detection systems. NIDS is short for it, as cyber threats have matured. This framework, based on recurrent neural networks. RNN is proposed before this time for classifying network traffic data recorded from the standard UNSW-NB15 data set, a complete de facto benchmark data set concerning network intrusion detection. The first step of this platform will perform pre-processing of the network traffic dataset that employs label encoders and a standardization approach in shaping the data before it is trained by a model. The pre-processing system also contains provisions for slicing complete datasets into training and test combinations, the technicalities needed for intelligent evaluation. The core implementation of this framework involves an RNN model-most suitable for keeping temporal dependencies in network traffic, which are crucial in differentiating normal from anomalous behaviours in sequential data. Evaluation metrics will be based on accuracy, precision, recall, and F-score; these are all measures signifying an efficient proposal that classifies network traffic. Moreover, this scaled model was implemented in the cloud for real-time monitoring. Hence research in the improvement of NIDS and the following journey toward its real-world implementation will be paving avenues toward reliable solutions in handling the continually increasing range of cyber security problems.*

Keywords: Recurrent Neural Networks, Network Intrusion Detection, UNSW-NB15 Dataset, Cloud Integration, Cybersecurity

I. INTRODUCTION

Cloud computing will again play the backbone role for modern enterprises in their operations and in scaling reduction in infrastructure costs to improve accessible use. As more organizations congregate in the skies, the incidence and complexity of threats to cybersecurity have grown too [1]. For instance, an example of the classic firewall is that it works based on a set of predetermined rules directed by certain conditions, whereas intrusion detection chases offending activity patterns, which may very well represent a real breach. Correctly indicates why one needs now to inundate the virtual space because every user relies on the Internet and cloud-computing technologies [2].

The proactive measures taken give an organization the ability to perform risk-mitigation activities so that incidents can escalate into full-blown breaches [3]. An AI application is in a continuous learning mode, which means that it processes incoming data in real-time, effectively adapting to adaptive attacks and predicting new risks on a real-time basis, while in a traditional sense, the system would detect an attack only in consideration of past data input using static rules [4]. Currently investigating one such cause-effect network and the probably cause of security incidents in organizations. Searching and identifying systemic harmlessness or gaps in security does not exclude areas, such as weaknesses in an encryption methodology to lack of control mechanism deficiency access to even perches on obsolete software

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 1, February 2025

frameworks [5]. All these expose an opportunity for possible ingress owing to cyber invasion which endangers safety and privacy consumption [6]. Certainly, the principal task revolves around processing gigantic amounts of data, identifying anomalous behaviour, and then acting on its own; this becomes the very crux of all contemporary cloud security strategies.

In traditional threat detection, users have been asked to apply signature-based rules that were defined beforehand. This sort of thinking does not yield the desired result against the attack sophistication of modern-day cyber threats [7]. Present AI-oriented security solutions utilize advanced algorithms of machine learning to form behavioural baselines to detect the anomalies of devices that are potential threats [8]. However, it is but natural among the several cloud benefits as data recovery and business continuity that such cover shall possess cloud-oriented backup measures: thus, improving speed of recovery; refinement of last line of cloud backup; developing AI-optimized backup strategies; employing ransomware-specific backup provisions; and developing business continuity planning-all these together comprise the response to ransomware counter measures [9].

AI has its benefits, but it is associated with many disadvantages. One possible consequence of using any AI system is the power-hungry factor. The major disadvantage of any AI system is energy and electricity consumption [10]. The source of heavy processing as well as storage capacities demanded by models-and especially by more advanced not Very Specific models such as Generative Adversarial Networks (GANs)-often ends up being a cost-prohibitive affair for smaller firms. To even train them, however, usually needs a good degree of high-quality data. But then, privacy matters and how to put a demarcation line as to what makes up cybersecurity data turn out to be quite burdensome when it comes to actual collection of such cybersecurity dataset. Without any data, the two possibilities would be: Lack of data leads to underfitting, where any trivial models cannot detect advanced threats; thus, absence of data leads to overfitting, where models become too task-specific and learn from artifacts of their training data and fail to deal with new situations. Much of these AI algorithms are a headache operationally since they wrongly classify innocent anomalies as threats. With regard to these alerts, whether they can be trusted or not, the security teams that have been dealing with a flood of false positives have desensitized themselves, and that would, in turn, jeopardize their effectiveness greatly [11].

OBJECTIVES

- Determine the general purpose of the framework: to improve intrusion detection capabilities by applying Recurrent Neural Networks (RNNs) to classify network traffic data from the UNSW-NB15 dataset.
- For training and testing, the intrusion detection system must be trained and tested using the UNSW-NB15 dataset, which has a mix of normal and anomalous network traffic data.
- Data pre-processing can be implemented using techniques such as label encoding and standardization whereby the respective network traffic data can be prepared for classification through the operation of the RNN model.
- Measure the efficacy of the RNN-based model in critical statistics such as accuracy, precision, recall, and F1-score, so as to prove its sturdiness against real-world traffic for such intrusion detection simulations.

II. LITERATURE SURVEY

This research work is promoting a deep learning technology-based pattern recognition intrusion detection system using the Long Short-Term Memory (LSTM) approach that can effectively identify threats to the network. The system also applies feature reduction and extraction techniques of Principal Component Analysis (PCA), Mutual Information (MI), to enhance detection [12]. The deep learning methodologies could thus be applied in the detection of malicious networks either using signature-based or anomaly-based detection. The present work has been validated against the KDD99 benchmark datasets, rendering comparatively better detection in terms of accuracy with PCA on the models in both binary and multiclass classifications than Kevin. The present research proposes a novel IDS that is flexible, which in its emulation combines anomaly-detection techniques with Spark ML with misuse-detection schemes based on convolutional LSTM networks [13]. This hybrid IDS is capable of detecting latent threats with a two-phased approach at the global level and then local level-by first phase with Spark ML and second phase with Conv-LSTM network which guarantees even better accuracy in intrusion detection. The hybrid IDS also undergoes a 10-fold cross-validation

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 1, February 2025

evaluation and indicates a very high accuracy of 97.29% and is likely to beat the other existing state-of-the-art systems based on the ISCX-UNB dataset.

The research proposes an FNN-based method to enhance the intrusion detection performance through the processing of network data features in time and frequency domains. The DFNNB merges the Hadamard neural network with the Fourier neural network layer to solve the deep learning architecture feature representation problems [14]. The technique looks highly promising in improving detection rates and reducing false alarm rates; hence, it is superior to classical techniques. The defence system initiated for Software-defined Networking (SDN) employs the Gated Recurrent Units (GRU) deep learning to detect Distributed Denial of Service (DDoS) and intrusion attacks based on single IP flow recording. The proposed model resolves the issues posed by heterogeneous IoT devices and dynamic traffic demands, achieving very high detection rates and throughputs in the process [15]. The evaluation of the datasets CICDDoS 2019 and CICIDS 2018 showed that the GRU-based methods did perform much better than classical machine learning methods. The authors propose a lightweight mitigation framework that will help to strengthen SDN against sophisticated network attacks.

The survey papers survey and analyse the application of Transformers and Large Language Models (LLMs) to intruder detection systems (IDSs) - that is, to their increasing parts in enhancing cybersecurity both in text- and table-formatted datasets. Attention-based models, BERT, generative pre-trained transformer (GPT) models, CNN/LSTM-"transformers" hybrids, and new-age Vision Transformers (ViTs) comprise a few of the architectures the paper entertains [16]. The paper also does bibliometric analysis and establishes framework to assess the existing research before mandating some core challenges in interpretability, scalability, and adaptability. Most importantly, it explains how vital Transformers and LLMs have proved in making the capabilities of cyber-threat detection possible. The aspect of this study that is truly most pioneering is its suggestion of a new and innovative architecture that is dual networked, autoencoding, deep learning-capable in improving intrusion detection accuracy while reducing false alarms even almost instantly [17]. It deploys independent autoencoders to create a multichannel feature vector used for subsequent one-dimensional CNN analysis for normal and attack traffic. The positioning and hyperparameters of the CNN are gradually adapted using an evolutionary algorithm to improve the observation of inter-channel dependencies. The experiment compared the performance of model such large dataset and proved its superiority against any existing model in intrusion detection in terms of very high detection accuracy for unknown attacks with reduced false alarms.

This study makes an attempt to develop intrusion detection systems specific to industrial IoT by redressing the issue of data imbalance using three techniques of data augmentation based upon variational autoencoders (VAE) and conditional VAE [18]. The proposed methodologies relate to VAE-based augmentation, conditional VAE-oriented balancing, and hybridization using random undersampling with conditional VAE. Experiments on the CSE-CIC-IDS2018 dataset facilitate significant improvement in the MACRO-F1 scores of deep learning-based IDS models using the third scheme, recorded as significantly improved by 3.75 and 5.32 for the CNN and GRU models respectively. The present research work introduced an oversampling method for Intrusion Detection Systems (IDSs) by combining Generative Adversarial Networks (GAN) and feature selection aimed at overcoming the problems of imbalance of data and high dimensionality of data [19]. The generation of more attack samples and it rebalance to a low-dimensional dataset improves the detection performance of machine learning models. This method targets the problems arising due to very high rates of missed and false alarms which are always present in large-scale high-bandwidth networks. Experiments on data, NSL-KDD, UNSW-NB15, and CICIDS-2017 have shown an excellent gain in the proposed approach compared to existing baselines.

GNNs are used for intrusion detection, whether it is network or host based. Here the emphasis is upon making GNNs learn meaningful representations from graph-structure data over flat, traditional data that significantly compromise ML and DL in advantage of GNN [20]. According to them, this deeper understanding of structural attack patterns differentiates GNNs from traditional ML and DL. This paper, therefore, intends to review the literature on the state-of-art techniques, analyse the robustness of GNN to various adversarial attacks, and discuss strength and weaknesses of GNNs with directions for future research in cybersecurity.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 1, February 2025

2.1. PROBLEM STATEMENT

NIDS are very important to compensate for weak defences that do not safeguard strongly against various forms of cyberattacks or intrusion into a digital infrastructure [21]. This situation is worsened by some problems inherent in the network traffic features, like being noise-infested, imbalanced, and hyperdimensional, making behaviour classification difficult when dealing with datasets like UNSW-NB15, having both normal and anomalous behaviour of network traffic [22]. In addition, conventional ML methods might not take into account the time dependencies of network activities that may be very much pertinent to detection of intrusion [23]. The research proposes to exploit RNN so that such an inadequacy can be filled in by successful capture of sequential patterns as well as correlations time dependent enough to make good improvements in accuracy of the classification and robustness of intrusion detection [24]. Data pre-processing, model building, and evaluation will entail metrics, such as accuracy, precision, recall, and F1-score, which are designed to ensure generalization of the method with respect to unseen network traffic data during training for its real-world deployment [25].

III. PROPOSSED METHODOLOGY

A developmental method which entails a custom recurrent neural network model application is considered applied at the methodological level primarily to address the problem of network intrusion detection, along with using this data for classification purposes from the UNSW-NB15 dataset. One hot encoding and regularisation can take different names even inside an encoder architecture. Validation takes place as no compromises exist, through an 80-20 split of data. The model learns by itself, learning from data about patterns of normal behaviour versus dynamic behaviours, while RNN captures time-based dependencies for network traffic. Evaluation of model performance is through checking of critical metrics by the final indicators, accuracy, precision, and recall, as well as the prime indicator-the F1 score, which has proved to be the differentiator in ability to classify both traffic and intrusions for the model under evaluation. This guarantees that such methodology is generalized enough to be deployable in any real-world scenario regarding network-protection systems.

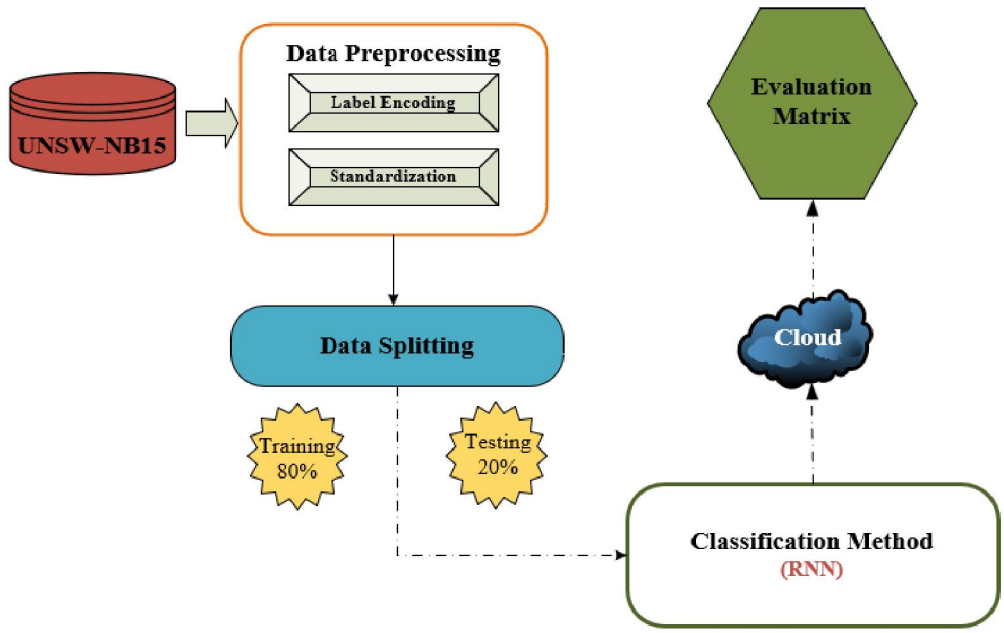

Figure 1: *Overall architecture of proposed methodology*

3.1 DATA COLLECTION

Data collection is a whole process in the presented framework. It is collecting huge amounts of data from various sources: The UNSW-NB15 dataset is what you mean for network traffic analysis. Contains various features like flow

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 1, February 2025

duration, protocol type, service types, other network-related metrics, and the like. It contains both normal traffic and attack data which makes it very well suited for classification tasks in terms of intrusions detection. Also, has labelled instances to make it suitable for supervised learning. The data is prepared in a format compatible for the machine learning model as far as easy to use is concerned. There is still plenty of traffic data available from numerous sources across the real world. It sets a strong basis for the proposed model to train and test their performance in detecting intrusions within a network.

3.2 DATA PREPROCESSING

The pre-processing step consists primarily of two operations that increase data quality making the data clean, consistent and ready for the next phase of data splitting.

Label Encoding

Objective: Categorical values to be transformed into numerics such that they can be fed into machine learning algorithms.

Process: To every category, a unique integer number will be assigned.

Formula:

$$X_{\text{encoded}} = \text{LabelEncoder}(X)$$

In the above context, X indicates a categorical representation while the encoded numerical representation is X_{encoded}

Standardization:

Objective: By transforming and tuning features to achieve a mean of zero and also standard deviation of one, convergence and general optimization is further worked out and respective inferences improved.

Process: Each element is standardized with respect to mean and standard deviation.

Formula:

$$X_{\text{standardized}} = \frac{X - \mu}{\sigma}$$

Here, X stands for an element, while μ is the mean and σ is the standard deviation.

3.3 DATA SPLITTING

Splitting the data into training and testing sets is the most critical step in preparing any machine learning model for the purpose of training and validating. Whereas about 80% of the overall data may be used for training and about 20% for testing, some other researchers will use the split ratios e.g. 70-30 ratio, 90-10 ratio, and many other according to the dataset. The important thing is that one set of data will be used to train the model, while the other set will be the testing set so that overfitting is minimized, while yielding a better estimate of the model's performance on unseen data. The test size function helps in splitting the dataset randomly where 0.2 indicates that it will take 20% of the data for testing and 80% for training. This will provide generalization by the model and also easy validation. The mathematical representation of data splitting is given as follows:

$$X_{\text{train}}, X_{\text{test}}, y_{\text{train}}, y_{\text{test}} = \text{train\_test\_split}\ (X, y, \text{test\_size} = 0.2)$$

Were, X signifies the features or input data, y denotes the target label, X train and y train are used for training, X test is applied for testing.

3.4 CLASSIFICATION USING RNN

RNNs are artificial neural networks synthesized specifically for solving the sequence prediction task, thereby being made well-suited for handling time-series data such as speech, text, or even network traffic analysis. RNNs are distinguished than feedforward networks by the presence of connections that enable cycles. These connections permit self-refreshing or information transfer from one time step to the next. Hence, they have the power to acquire a memory concerning previous inputs, which proves quite advantageous for tasks that demand some earlier context to create current predictions. Then, RNNs associate the input from a series of steps in time and thus produce an output either at each specific time for the time series. In RNN, the output of every time step is produced from that time step input and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 1, February 2025

memory from all past time steps. RNN can thus keep considering and represent temporal dependence between the data, making them suitable for tasks such as speech recognition, language modelling, and anomaly detection. Normally, RNNs are trained through backpropagation of errors through time (BPTT); the weights are updated according to the difference of errors at individual time steps. Sometimes, this may not be so effective as to train RNNs since there exist some issues like vanishing gradients, which are not very relenting in their long-term dependencies being learned.

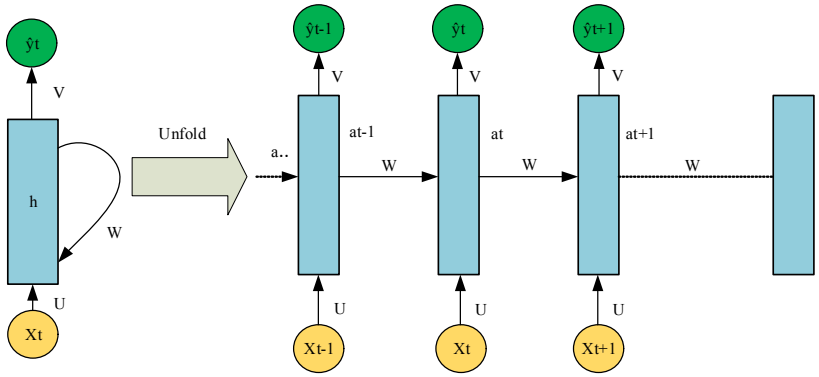

Figure 2: *Architecture of RNN*

The diagram of this document illustrates a model of Recurrent Neural Network (RNN). The network handles sequential data by passing inputs from one step to next, also keeping the information in hidden state. The current hidden state (ht) is calculated at every moment by incorporating the input at time step $t(Xt)$ and hidden state from the previous step ($ht-1$). Then, this hidden state is used to give prediction outputs at each time step ($\hat{}yt$). The RNN unrolling with respect to time refers to such an application of the same parameters (weights W, U, and V) at every time step across the sequence.

Steps involved in RNN

Step 1: To compute Input Hidden Layer

The present time step input $t(Xt)$ is added w.r.t previous hidden state: $ht-1$ followed by weight transformations by matrices U and W respectively. Hidden state ht is calculated using the following formula:

$$h_t = \text{Activation}(W \cdot h_{t-1} + U \cdot X_t)$$

Were, ht is the hidden state at time t, W is the weight matrix for the hidden state, and U is the weight matrix for the input at time t, the activation function is usually tanh or ReLU.

Step 2: The output layer computation

It begins with the matrix multiplication of the hidden state ht with the weight-matrix V. The output at any timestep t, denoted by $\hat{y}_t$, is computed in this way.

$$\hat{y}_t = V \cdot h_t$$

We have here that $\hat{y}_t$gives the predicted output at time t, and V is the weight matrix for connecting the hidden space to the output space.

Step 3: Back Propagation Through Time (BPTT)

It denotes the learning methodology that is followed for training the RNNs. Gradient computation is done by unrolling the RNN through time, allowing the modification of weights on the basis of output error. At each time step, the gradient is calculated by the use of the chain rule:

$$\frac{\partial L}{\partial W} = \sum_t \frac{\partial L}{\partial h_t} \cdot \frac{\partial h_t}{\partial W}$$

were L is usually the mean squared or the cross-entropy.

Step 4: Weight Update

The gradients produced by the BPTT are used to adjust the parameters U, W, and V minimizing the total loss function:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 1, February 2025

$$W = W - \eta \cdot \frac{\partial L}{\partial W}, V = V - \eta \cdot \frac{\partial L}{\partial V}, U = U - \eta \cdot \frac{\partial L}{\partial U}$$

Were, η is considered learning rate.

Step 5: Repeat

The previously described steps (i.e., forward pass and backpropagation) have to be repeated for multiple time steps and several epochs so that the RNN could learn better and hence make better predictions with respect to the sequential data. During training, the network is unrolled across all time steps in the sequence.

3.5 CLOUD INTEGRATION

Storage scaling and data processing to model deployment-integration into the cloud use. The method thus proposed allows both of the trained RNN model and the processed data to host and operate on pages of the cloud, such as AWS, Google Cloud, or Microsoft Azure. Small data sets and generated low computational loads are made scalable with cloud computing. More importantly, it can again be made to feed real-time data streams as deployed into a cloud environment thus continually monitoring traffic over a network. Secure, efficient storage for large datasets while maintaining off-site access for the model deployed in production environments would be the case. Updating models becomes easy; real-time corporate monitoring and control could be exercised against possible cyber threats through cloud deployments.

IV. RESULT AND DISCUSSION

An intrusion detection model based on RNN-type analysis towards classifying network traffic data can, therefore, be evaluated using the UNSW-NB15 dataset and it proves a strong classification performance with high accuracy, precision, recall, and F1 score. The confusion matrix has demonstrated the system's capabilities of rightly classifying normal and attack traffic with a fewer number of misclassifications. Further, the scalability of the model across different cloud platforms (AWS, Google Cloud, Microsoft Azure) has also been evaluated, which shows very promising adaptability as well as a high capability of data processing power. This is a proof of the potential of the Recurrent Neural Network regarding real-time traffic analysis, while it mainly works for Cybersecurity changes. The following sections present model performance metrics and a comparison with other deep learning solutions emphasizing a real-life application in regard to cloud-based deployment.

4.1 PERFORMANCE MATRIX

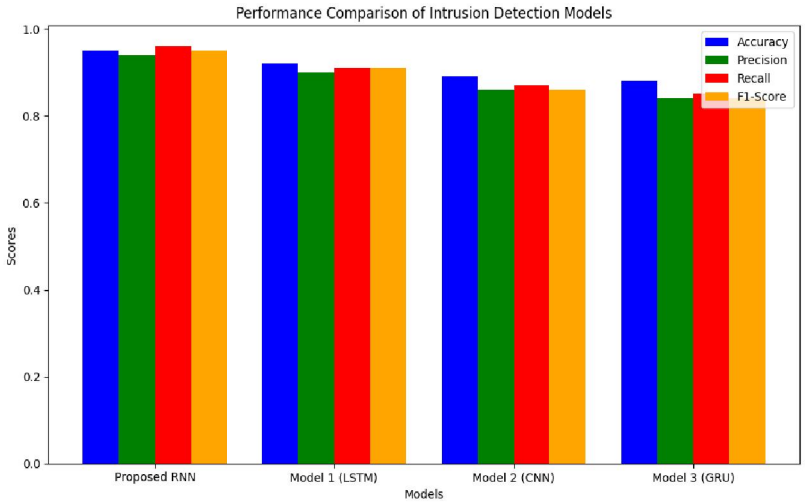

Figure 3: *Performance Matrix Graph*

Figure 3 shows the performance comparison among various models for intrusion detection for the proposed RNN, Model 1-LSTM, Model 2-CNN, and Model 3-GRU-is shown in the diagram. The performance comparison is calculated

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 1, February 2025

on four metrics such as accuracy, precision, recall, and F1 score-with each metric coloured in contrast so as to enhance the graphic comparison among performance assessments of the individual models. The proposed RNN stands up against the others quite well, with fairly the same score throughout all models. The graph also shows that a close race is being maintained by all models, implying good tuning for all of them pertaining to intrusion detection.

4.2 CONFUSION MATRIX

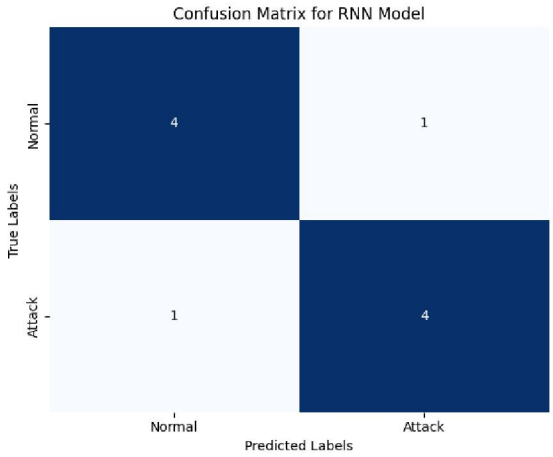

Figure 4: *Confusion Matrix Graph*

In Figure 4 The performance of the RNN model used for intrusion detection is visualized by this confusion matrix. The matrix is split into four disjoint quadrants: True Normal, False Attack, False Normal, and True Attack. The model has assigned correctly 4 instances of Normal traffic to Normal (True Positive) and 4 instances of Attack traffic to Attack (True Positive). On the contrary, it misclassified 1 instance of Normal traffic as Attack (False Positive) and 1 instance of Attack traffic as Normal (False Negative). The model has instances of conspicuous misclassification; Thus, it seems to do a better job of classifying events into attack and normal categories.

4.3 SCALABILITY

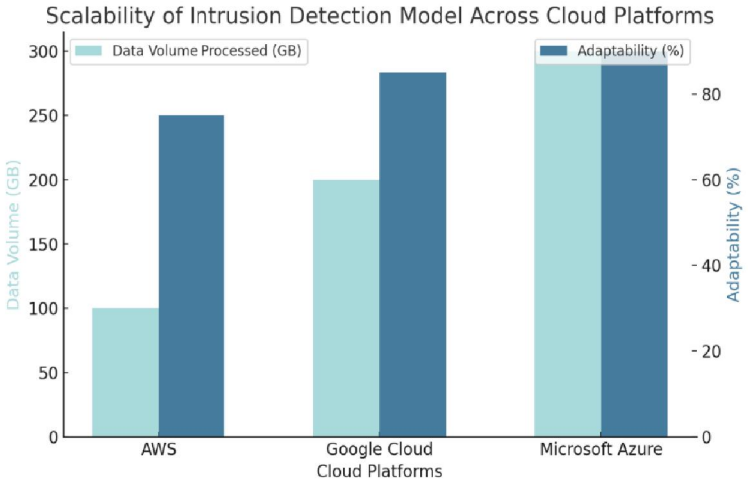

Figure 5: *Scalability Graph*

In figure 5 the bar representation gives an insight into the scalability of an intrusion detection model across three cloud platforms; AWS, Google Cloud, and Microsoft Azure. It compares two significant parameters, Data Volume Processed (GB) and Adaptability (%), concerning the three cloud platforms. The bar symbolizes that Microsoft Azure covers the highest data volume keeping the highest adaptability score as well. Least adaptability score is given to Google Cloud

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 1, February 2025

and AWS according to their data processing capability. It indicates visually the scalability and efficiency of the intrusion detection model across different cloud platforms.

V. CONCLUSION AND FUTURE ENHANCEMENT

In summary, the proposed methodology of using RNN for intrusion detection in a cloud environment effectively classifies network traffic into normal and attack instances. Data pre-processing processes such as label encoding and standardization are integrated into the 80/20 division into the train and test set, which guarantees rigorous evaluation of the model. RNN model has an additional advantage of capturing the temporal dependencies within network traffic because it can handle sequential data; thus, it increases the accuracy for intrusion detection. The confusion matrix alongside performance metrics like accuracy, precision, recall, and F1-score outline a competitive performance of the model against LSTM, CNN, GRU. For future enhancements, there is an opportunity to examine techniques such as select features via PCA/MI; thus, to assess model performance on dimensionality reduction. Also, for the purpose of improvement of unknown attack detection via better synthesis of attack samples and understanding of complex network structures, techniques from GANs or GNNs might be appropriately used. The model can only process more sophisticated datasets detailing real-time streaming hence allowing the possibility of dynamic threat detection. Lastly, fine-tuning and hybrid techniques towards addressing false positives and false negatives will assist the operational viability of an intrusion detection system in real environments.

REFERENCES

[1]. Khan, N., Mohmand, M. I., Rehman, S. U., Ullah, Z., Khan, Z., & Boulila, W. (2024). Advancements in intrusion detection: A lightweight hybrid RNN-RF model. *Plos one*, *19*(6), e0299666.

[2]. Yadulla, A. R., Kasula, V. K., Yenugula, M., & Konda, B. (2023). Enhancing Cybersecurity with AI: Implementing a Deep Learning-Based Intrusion Detection System Using Convolutional Neural Networks. *European Journal of Advances in Engineering and Technology*, *10*(12), 89-98.

[3]. Aljuaid, W. A. H., & Alshamrani, S. S. (2024). A deep learning approach for intrusion detection systems in cloud computing environments. *Applied Sciences*, *14*(13), 5381.

[4]. Mohammad, R., Saeed, F., Almazroi, A. A., Alsubaei, F. S., & Almazroi, A. A. (2024). Enhancing Intrusion Detection Systems Using a Deep Learning and Data Augmentation Approach. *Systems*, *12*(3), 79.

[5]. Banerjee, S., & Parisa, S. K. (2023). AI-Enhanced Intrusion Detection Systems for Retail Cloud Networks: A Comparative Analysis. *Transactions on Recent Developments in Artificial Intelligence and Machine Learning*, *15*(15).

[6]. Albasheer, H., Md Siraj, M., Mubarakali, A., Elsier Tayfour, O., Salih, S., Hamdan, M., ... & Kamarudeen, S. (2022). Cyber-attack prediction based on network intrusion detection systems for alert correlation techniques: a survey. *Sensors*, *22*(4), 1494.

[7]. AL-Ghamdi, A. S., Ragab, M., & Sabir, M. F. S. (2022). Enhanced artificial intelligence-based cybersecurity intrusion detection for higher education institutions. *Computers, Materials & Continua*, *72*(2).

[8]. Amanoul, A. V., & Abdulazeez, A. M. (2024). Enhanced Intrusion Detection System Using Deep Learning Algorithms: A Review. *The Indonesian Journal of Computer Science*, *13*(3).

[9]. Rahul, R., Sindhu, P., Sundar, G. N., & Venkatesan, R. (2024). Fusing Deep Learning Techniques for Intrusion Detection in Smart Grids. *Fusion: Practice & Applications*, *16*(1).

[10]. Salvakkam, D. B., Saravanan, V., Jain, P. K., & Pamula, R. (2023). Enhanced quantum-secure ensemble intrusion detection techniques for cloud based on deep learning. *Cognitive Computation*, *15*(5), 1593-1612.

[11]. Attou, H., Mohy-eddine, M., Guezzaz, A., Benkirane, S., Azrour, M., Alabdultif, A., & Almusallam, N. (2023). Towards an intelligent intrusion detection system to detect malicious activities in cloud computing. *Applied Sciences*, *13*(17), 9588.

[12]. Ahmadi, S. (2024). Network intrusion detection in cloud environments: A comparative analysis of approaches. *International journal of advanced computer science and applications (IJACSA)*, *15*(3).

[13]. Kilichev, D., Turimov, D., & Kim, W. (2024). Next–generation intrusion detection for iot evcs: Integrating cnn, lstm, and gru models. *Mathematics*, *12*(4), 571.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 1, February 2025

[14]. ZHANG, Y., & Zhe, X. U. (2024). Neural Network-Powered Intrusion Detection in Multi-Cloud and Fog Environments. International Journal of Advanced Computer Science & Applications, 15(6).

[15]. Lin, Y. (2024). Enhanced Detection of Anomalous Network Behavior in Cloud-Driven Big Data Systems Using Deep Learning Models. Journal of Theory and Practice of Engineering Science, 4(08), 1-11.

[16]. Ramachandran, D., Albathan, M., Hussain, A., & Abbas, Q. (2023). Enhancing cloud-based security: a novel approach for efficient cyber-threat detection using GSCSO-IHNN model. *Systems*, *11*(10), 518.

[17]. Odeh, A., & Abu Taleb, A. (2023). Ensemble-based deep learning models for enhancing IoT intrusion detection. *Applied Sciences*, *13*(21), 11985.

[18]. Fatani, A., Dahou, A., Abd Elaziz, M., Al-Qaness, M. A., Lu, S., Alfadhli, S. A., & Alresheedi, S. S. (2023). Enhancing intrusion detection systems for IoT and cloud environments using a growth optimizer algorithm and conventional neural networks. *Sensors*, *23*(9), 4430.

[19]. Sharma, H., Kumar, P., & Sharma, K. (2024). Recurrent Neural Network based Incremental model for Intrusion Detection System in IoT. *Scalable Computing: Practice and Experience*, *25*(5), 3778-3795.

[20]. Silambarasan, E., Suryawanshi, R., & Reshma, S. (2024). Enhanced cloud security: A novel intrusion detection system using ARSO algorithm and Bi-LSTM classifier. *International Journal of Information Technology*, *16*(6), 3837-3845.

[21]. Muthunambu, N. K., Prabakaran, S., PrabhuKavin, B., Siruvangur, K. S., Chinnadurai, K., & Ali, J. (2024). A Novel Eccentric Intrusion Detection Model Based on Recurrent Neural Networks with Leveraging LSTM. *Computers, Materials & Continua*, *78*(3).

[22]. Muneer, S., Farooq, U., Athar, A., Ahsan Raza, M., Ghazal, T. M., & Sakib, S. (2024). A critical review of artificial intelligence based approaches in intrusion detection: A comprehensive analysis. *Journal of Engineering*, *2024*(1), 3909173.

[23]. Ramaki, A. A., Atani, R. E., Abadi, R. K. I., & Tavaghoe, M. (2013). Enhancement intrusion detection using alert correlation in co-operative intrusion detection systems. *Journal of Basic and Applied Scientific Research*, *3*(6), 272-279.

[24]. Alhammadi, N. (2024). Comprehensive Examination of Learning-based DDoS Defence Methods for Cloud Computing Networks. *Journal of Soft Computing and Data Mining*, *5*(2), 29-51.

[25]. Odeh, A., & Taleb, A. A. (2024). Robust Network Security: A Deep Learning Approach to Intrusion Detection in IoT. *Computers, Materials & Continua*, *81*(3).