Iraqi Journal of Statistical Sciences

https://stats.mosuljournals.com/

Innovative Cloud Security Solutions: Hybrid RNN and CNN Models for Intrusion Detection

Ahmed Akbar Muhammad

Azad University Tehran, Tehran, Iran

Article information

Article history:
Received July 1, 2024
Accepted August 25, 2024
Available online December 1, 2024

Keywords:
Cloud Security
Intrusion Detection Systems
Deep Learning
Recurrent Neural Networks
Convolutional Neural Networks
Cyber Threats Detection

Correspondence:
Ahmed Akbar Muhammad
kahmed833@gmail.com

Abstract

Cloud computing infrastructures have moved to the very heart of global business operations, which also places them in prime position for numerous advanced cyber threat challengers. This makes traditional predefined rule-based and known signature-based intrusion detection systems (IDS) almost useless in this era of advanced threats, including zero-day attacks, APTs - Advanced Persistent Threats exploiting polymorphic malware. The paper introduces a revolutionary hybrid model which uses the power of Recurrent Neural Networks (RNN) and Convolutional Neural Networks (CNN) to evolve cloud-based Intrusion detection system. This hybrid method uses the RNN to encode and learn from time-series data, acquiring memory over temporal anomalies in information; besides this it makes extensive use of Convolutional neural networks for spatial feature extraction at high-throughput which becomes essential for detecting these patterns across multitudes that suggest intrusions. In well-defined cloud setting, The overall effectiveness of this model is assessed by testing it under numerous attack scenarios. The results indicate that this model not only outperforms standard IDS in terms of detectio. but also demonstrates outstanding resilience against zero-day and emergent threats. This increased detection efficiency is obviously necessary to ensure the security and reliability of cloud services, allowing more stringent defense mechanisms which remains essential in modern dynamically evolving cyber threat landscapes

DOI: 10.33899/iqjoss.2024.185233

1. Introduction

With an emphasis on the developments of cyber era, cloud computing has become a key to modern business operation where it provides scalability and flexibility efficiency [1]-[4]. But as usage of cloud-based environments grows, so does the appeal from a cyber-threat perspective. These environments are by nature dynamic, distributed and prone to a variety of sophisticated attacks for which traditional security controls typically fail.

In order to protect such environments, Intrusion Detection Systems (IDS) [5][6] play a key role as they keep monitoring the network traffic so that it can alert if any malicious activities are detected. While traditional IDS solutions mainly use pre-defined rules (signatures) for detecting intrusion. Such techniques are good at protecting against known threats but no longer practical when confronted with zero-day vulnerabilities, polymorphic malware and volumetric distributed denial of service(DDOS) attacks (all common throughout modern cloud-based systems).

In this study various common and emerging cyber-attacks, such as Denial of Service (DoS), Distributed Denial of Service (DDoS) and ransomware attacks. These attacks were selected to be increasingly common in cloud and IoT environments, hence being vital threats to mitigate with advanced intrusion detection systems.

In this research paper a new convolutional approach based on Recurrent Neural Networks(RNN) and Convolutional Neural Network has been used to increase the potential of Intrusion Detection Systems in cloud environments[7]. This hybrid model makes use of both RNNs to capture and forecast patterns over time, together with the ability for spatial feature extraction from data flows which is well handled by CNNs. Thus, this architecture combines both networks to detect not just the known types of intrusions but also discover anomalous patterns that could be a new untouched attack.

The rationale for an IDS this sophisticated is the fact that more and more of the cyber threats are automated, so it must be on par. Further machine learning models deployed such as the one suggested in this paper are able to learn from new data that it receives, allowing itself to update its threat detection abilities without manual updates of their databases. In cloud environments where the threat landscape can change quickly, this is especially advantageous.

Finally, The hybrid RNN-CNN model introduced represents a significant advancement in security, facilitating the development of more precise recognition models that enhance cloud infrastructure defense against a wide range of cyber threats. This paper explores the architecture thoroughly and demonstrates its effectiveness from all perspectives, paving the way for a new security paradigm characterized by dynamic, intelligent, and robust intrusion detection.

2. Related Work

Intrusion detection systems (IDS) work through multiple methods to weed out anomalies leveraging algorithms as diverse in their implementation from data mining, machine learning and statistical approaches. There are researchers that studied the IDS's performance by investigating singular algorithmic approaches [8] and others motivate a hybrid methodology to improve on an exact issue in IDSs, however not much has been done so far. For example, Atefi et al. used a combination of genetic algorithms and support vector machines (SVM) for anomaly detection, where support vector machines (SVM) becomes more specific in precision compared to the use of an SVM only while further performance improvements were achieved when both approaches are combined into one hybrid Intrusion detection systems (IDS) [9].

Research by Khoei et al. applied three ensemble learning approaches such as bagging, boosting and stacking to anomaly detection problems tested them on data samples that are noisy using decision trees,naıve bayes, and K-nearest neighbors traditional solutions. In summary, their work showed that recognition rates using stacking-based approaches clearly outperformed those based on a single method [14].

At a classification level, Rakshe and Gonjari employed support vector machines (SVM) as well random forest approach to obtain accuracies greater than 95% in some cases using the NSL-KDD dataset. Such comparison is random forest performed better than SVM in traffic classification [11]. Kumar et al. created an IDS using Naïve Bayes, ID3 (Iterative Dichotomiser 3) and (Multilayer Perceptron) MLP algorithms with ensemble learning in the CICIDS2017 dataset. In this case, the ID3 algorithm performed well above average in terms of precision (83.7), recall (82.54), accuracy (98) and F1 score [12].

Zhang et al. implemented an XGBoost-based misuse IDS for Local Area Network (LAN) individual using the real-time data obtained from 10 country users located in Asia [13]. Similarly, the study by Taher et al. proposed a signature-based IDS with Artificial Neural Network (ANN) and SVM implementation [14];

This problem has driven big cloud service providers (Amazon Web Service (AWS), Azure and Google) to use signature, behavioral as well machine learning detection techniques [15]. Gao et al. developed a novel malware detection model based on cloud semi-supervised learning, which includes a detection component built on a recurrent neural network (RNN) to ensure tenant privacy in public clouds [16].

Venkata Rao et al. recommended the Deep Wrap Neural Network (DLCNN) for detecting internet worms and NetFlow related to various attacks, assessing its effectiveness using PCAP and KDD-CUP-99 datasets [17]. Hasan Alkahtani and colleagues applied machine learning and deep learning techniques to detect malware in Android

systems, with SVM achieving the highest accuracy using the CICAndMal2017 dataset, and Long Short-Term Memory (LSTM) performing well on the Drebin dataset [18].

These studies collectively underline the potential and effectiveness of hybrid and machine learning approaches in enhancing the capabilities of IDS, setting a foundational backdrop for hybrid RNN-CNN model.

3. Methodology

The methodology of this study encompasses a series of integrated steps, starting from data collection to the detailed development and evaluation of various deep learning models specifically tailored for intrusion detection in internet of things (IoT) networks [19][20].

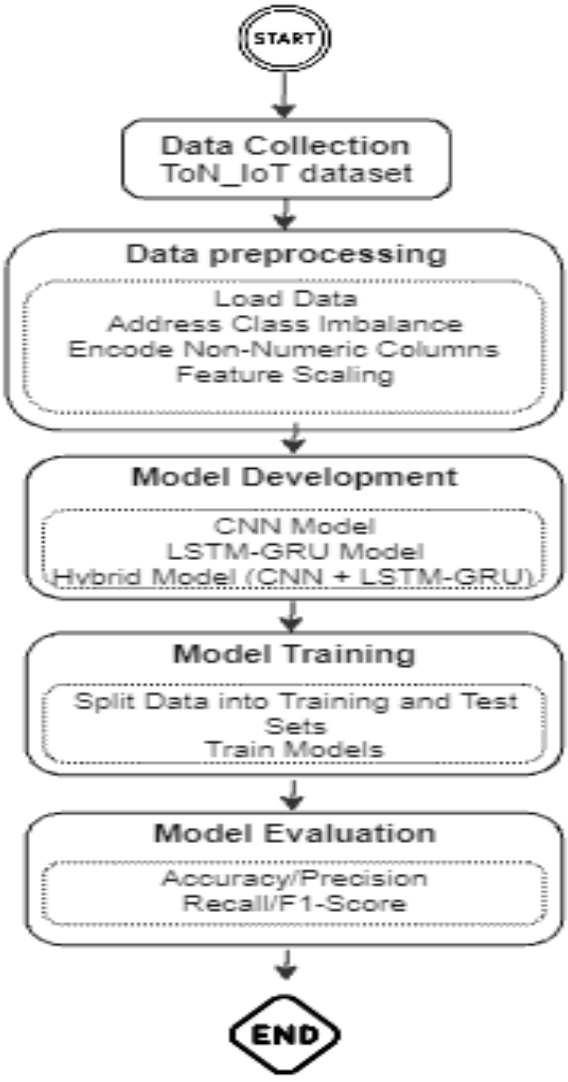

Figure 1.Proposed method

4. Data Collection

ToN_IoT [21][22]is designed as an extensive benchmarking resource to advance AI-driven cybersecurity solutions across IoT and IIoT (Industrial Internet-of-Things) environments; adopted in this study. This is home to a broad spectrum of data types that range from telemetry for numerous IoT and IIoT sensors, system logs (from Windows and Linux platforms), as well very precise records regarding network traffic. The name ToN stands for one of the types

Dataset it contains which is Telemetry, IoT and Network data so this made a wide range datasets to use in Cybersecurity research.

The dataset has been collected at a high-quality lab setup; Internet of Things (IoT) Laboratory in Cyber section, School of Engineering and Information Technology University of NSW(UNSW), Canbera based CDOT facility located within the Australian Defence Force Academy. In this, we have a larger scale Infrastructure 4.0 network with virtual machines (VMs), cloud infrastructure and Halcyon Resource Identifier in IoT Fog Computing environment deployed by various embedded type of sensors used for these kinds if infrastructure monitoring. Researchers to gather baseline operational data as well as a variety of cyber-attacks i.e., DoS, DDoS and ransomware attacks targeted at web application, IoT gateway and computing systems used this testbed.

This well-prepared dataset has its components stored in directories containing everything from training images to validation and model checkpointing. Raw data is collected from IoT/IIoT sensors, network traffic and all system logs of different types. To ensure universal use, the raw files has been converted into a common format such as CSV by our team for further exploratory analysis across different platforms. This dataset also provides a directory called "Train_Test_datasets" which is especially designed in order to train and test machine learning models for cybersecurity. In addition, "SecurityEvents_GroundTruth_datasets" contain timestamps and IP addresses for simulated attack events. This well-organized and detailed dataset offers a significant asset for developing AI-driven cybersecurity solutions, while accurately reflecting the conditions of future threats in IoT/ IIoT networks.

Moreover, ToN_IoT dataset is specially appropriate to train efficient intrusion detection models like the one constructed using an easy-to-use API of Spark MLLib. It consists of several kinds of network intrusions as well as normal behaviors, which makes it a great dataset to develop and evaluate secure networking solutions.

Types of Attacks Evaluated

For this study, models were tested against different types of cyber-attacks that are common and one emerging network attacks which pose a big threat to modern cloud and iot environments.

- Denial of Service (DoS): attacks attempt to make a network service unavailable by overwhelming it with an enormously high flood of illegitimate requests. This mass of requests is larger than the capacity resources (network, application) and leaves no space for a proper user request to respond. Such an attack is frequently employed to cripple websites, online services, or network resources significantly disrupting the operation time of organizations and incurring potential monetary and reputational loss.
- Distributed Denial of Service (DDoS): Distributed DoS attacks are a step-up from the previous type, more severe and complex. While DoS attacks come from one source, DDoS is when traffic floods in multiple sources and it can be orchestrated through millions of compromised devices and coordinated by botnet. Because of its distributed nature, DDoS attacks are more difficult to defend against since the malicious traffic surge comes from multiple locations in unison making it hard to distinguish and filter out or block without interfering with legitimate activity. DDoS attacks overload the availability of even enterprise-grade network infrastructures, and can turn a simple service internal outage to obvious operational issues.
- Ransomware: is a type of malware that is designed to block access to a computer system or data, typically by encrypting it, until the victim pays money. Typically, ransomware attacks get in through a system infection via phishing emails, malicious downloads or an exploitable network defense vulnerability. After, infecting a system it encrypts the sensitive files on that machine and then leaves behind a note stating ransom for an encryption key to decrypt those vital details. Ransom: This type of attack asks for a ransom to not permanently delete driving data. The ransomware has grown into one of the most infamous and devastating cyber-attacks that disrupts operations, interrupting not only those for individuals and businesses but also critical infrastructure by making financial losses.

As such, these particular attacks were selected as the focus due to their rapidly increasing number of times observed and level of complexity along with a severe impact on cloud / IoT environments. The principal of the threats that now needs to be managed by modern intrusion detection system is Denial-of-Service, Distributed-Denial-of-Service and Ransomware. It was chosen so that non financial brute force killing blow attacks are a testing methodology to check the developed models resilience and robustness against real life cyber threats.

The dataset used for this research consisted of simulations of these attacks, enabling the ultimate test bed in terms to both content and realism from those sort s detection models. These simulated attack scenarios injected into the models helped validate how well they could respond against real-life cyber threats and thereby, determine whether building a secure network operation around them to protect cloud or IoT systems was feasible. His complete evaluation process is designed to ensure that the models are both theoretically sound and effective in practice, able to protect digital infrastructures from threatening cyber attacks.

5. Data Preprocessing

The first step of data preprocessing was downloading and loading the dataset into a Pandas DataFrame[23]- [25], The imbalance in class distribution was addressed. The 'normal' class was significantly larger than the other classes, potentially resulting in a poor predictor that would consistently predict 'normal.' To mitigate this issue, downsampling was applied, reducing the number of normal samples to 20,000 and thereby balancing the dataset for training.

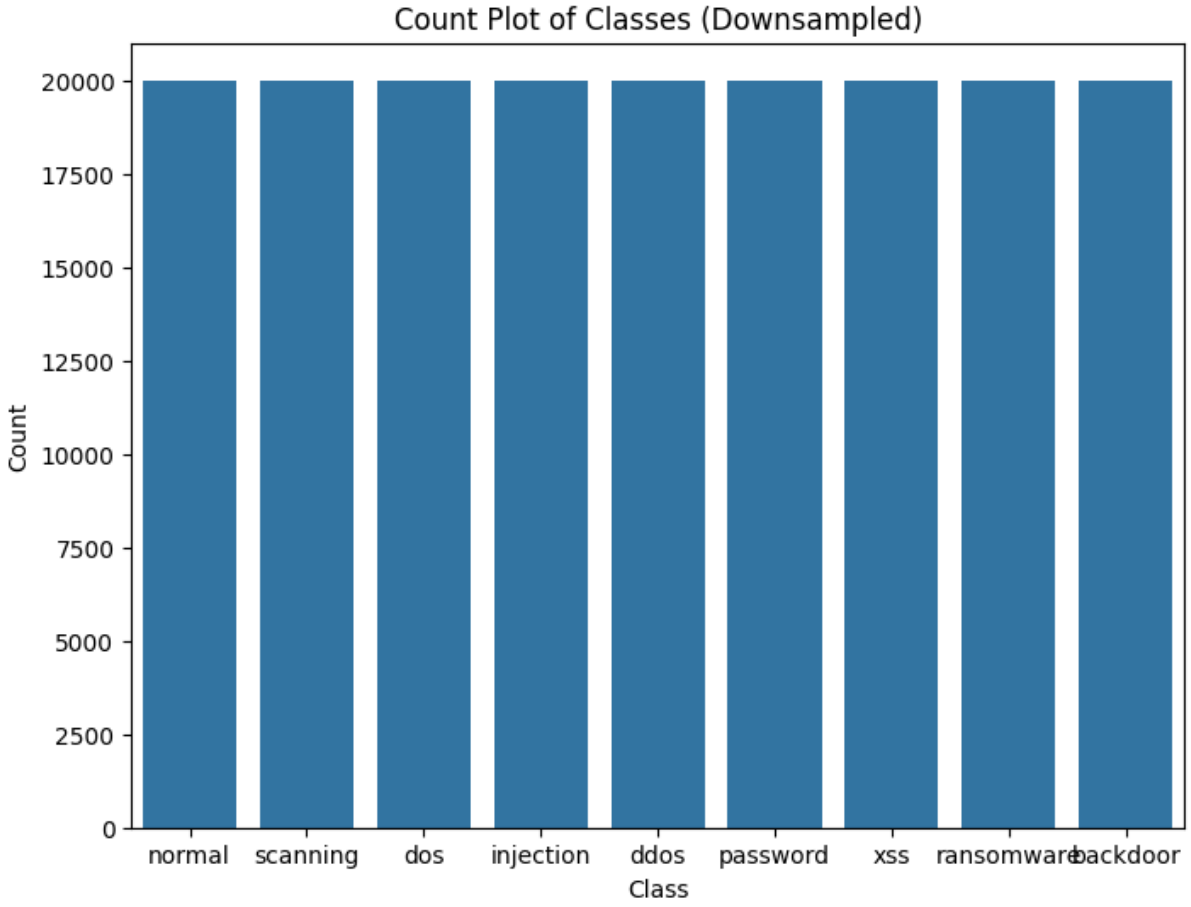

Figure 2 class down sampling

Next step in preprocessing phase is to change the non-numeric columns into Label encoding for further proceeding those with machine understanding format. This takes care of the other categorical data and makes it numerical. Moreover, feature scaling have done to make the values of features within a similar scale using MinMaxScaler[26][27] which assist in acceleration of learning for neural networks. One-hot encoding transforms the output variable 'type' into a binary matrix format, enabling its use as the target in the subsequent classification task.

6. Model Development

The research contributed three varied models to test their capability of intrusion detection:

The first model is a CNN Model and includes 1D convolutions. Useful when dealing with complex data, namely any spatial hierarchy. The architecture uses multiple layers: Conv1D and MaxPooling1D, ended by a Flatten layer with Dense layers. A dropout layer was added to prevent overfitting.

The second model is an LSTM-GRU [28]-[30] Model: The structure of this one contains a mix style version that uses some architectural layers based on the differences between both techniques. This architecture is meant to capture long-term and short-term dependencies respectively in data, which becomes necessary for detecting anomalies in sequential type of data such as network traffic.

The third model, which is a Hybrid Model that tries to take in the power of both first (CNN) and second (LSTM-GRU). It seeks to exploit the spatiotemporal feature learning capabilities for improved detection accuracy.

7. Model Training

All models were trained using the same dataset with an 80/20 training and test split to evaluate performance. Adam was used as the optimizer [31] with binary cross-entropy loss function [32, 33], given that this is a multi-class target variable. The model was trained for ten epochs with a batch size of 32 to achieve an optimal balance between improving the learning process and managing computational overhead.

8. Model Evaluation

These models were then evaluated by computing metrics like accuracy, precision, recall and F1-score. Confusion matrices were also used to visualize the performance of each model in classifying different types of network traffic. Sensitivity and specificity calculations were also performed to determine the models' ability to identify region-true positives (i.e., positively labeled as a given functional land cover) or true negatives for each grid cell into which Mexico was gridded.

Such approach was designed methodologically to test different model architectures as standalone models, and investigate the synergetic effect of combining various features in order to tackle a challenging problem - detecting intrusions on IoT networks.

Accuracy: This is the most straightforward performance metric, representing the ratio of correctly predicted observations to the total observations. It is particularly useful when the class distribution is balanced. The accuracy can be calculated using the following formula:

$$[\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{FN} + \text{TN}}]$$

Precision : is a metric that measures the accuracy of positive predictions made by a model, calculated as the ratio of true positives to the total positive predictions (true positives plus false positives). It's crucial when the cost of false positives is high.

$$[\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}]$$

Recall is a metric that measures the ability of a model to correctly identify all relevant instances in a dataset. It is calculated as the ratio of true positives to the sum of true positives and false negatives. High recall indicates that the model successfully captures most of the actual positive cases.

$$[\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}]$$

The F1 score is a metric that combines both precision and recall into a single value. It is the harmonic mean of precision and recall, providing a balance between the two. The F1 score is particularly useful when the cost of false positives and false negatives are both important to consider. It is calculated using the formula:

$$[\text{F1 Score} = \mathbf{2} \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}]$$

9. Results

This study is very significant in presenting the effectiveness of different variants of deep learning models [34] for intrusion detection in IoT networks. The data selected for the experiments was well-balanced, replicating class imbalances across different attack categories (scanning, denial of service -DoS-, injection) and normal traffic patterns.

Three different models CNN, LSTM-GRU and a hybrid model (combination of both) were evaluated after down sampling [35]-[38] followed by preprocessing. The key metrics used to measure each model's performance are Accuracy, Precision, Recall, and F1 Score.

10. Model Evaluation and **Performance**

CNN model shows awesomeness in these 4 matrixs 95% accuracy, 96% presicison,95% recall and 95% f1 score. They show how the CNN model is very powerful in the spatial features extraction, which is a very important in the identification of intrusion patterns in the network traffic.

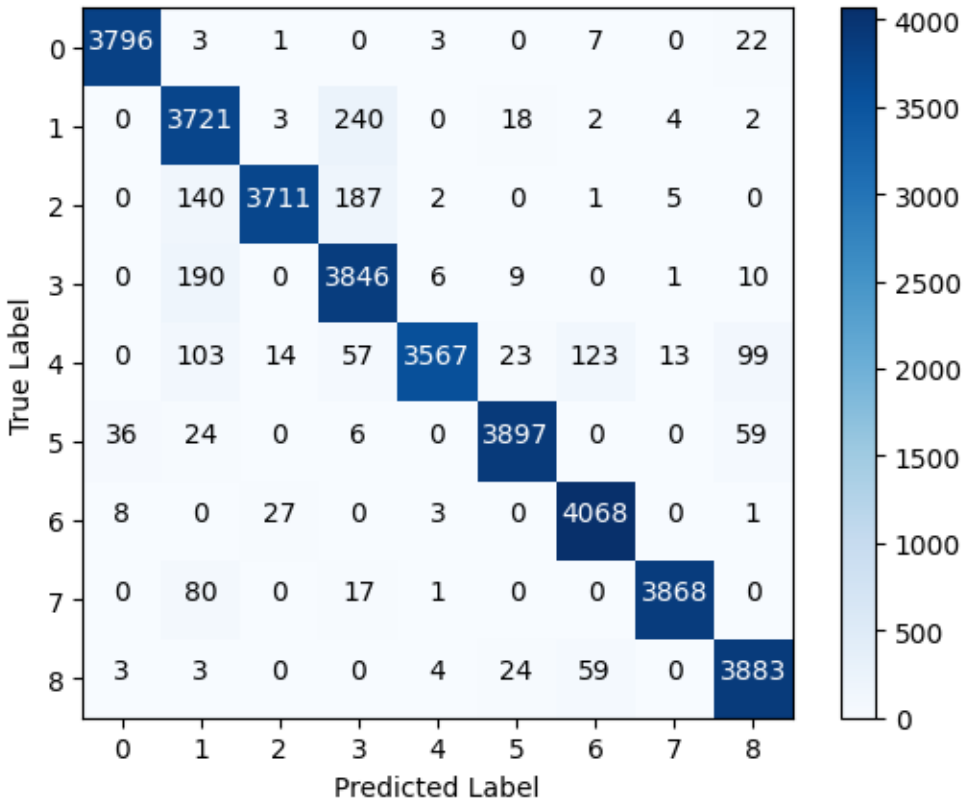

Figure 3 Confusion Matrix CNN

The LSTM-GRU model had the best performance for appropriately capturing temporal dependencies (98% accuracy), information precision and recall values, which were 98%, while the F1-score was also equal to! While this underpins its capability in addressing sequential data recognizing time-series [39] behavior across the network traffic and Ozdemir's more intricate intrusion attempts as well.

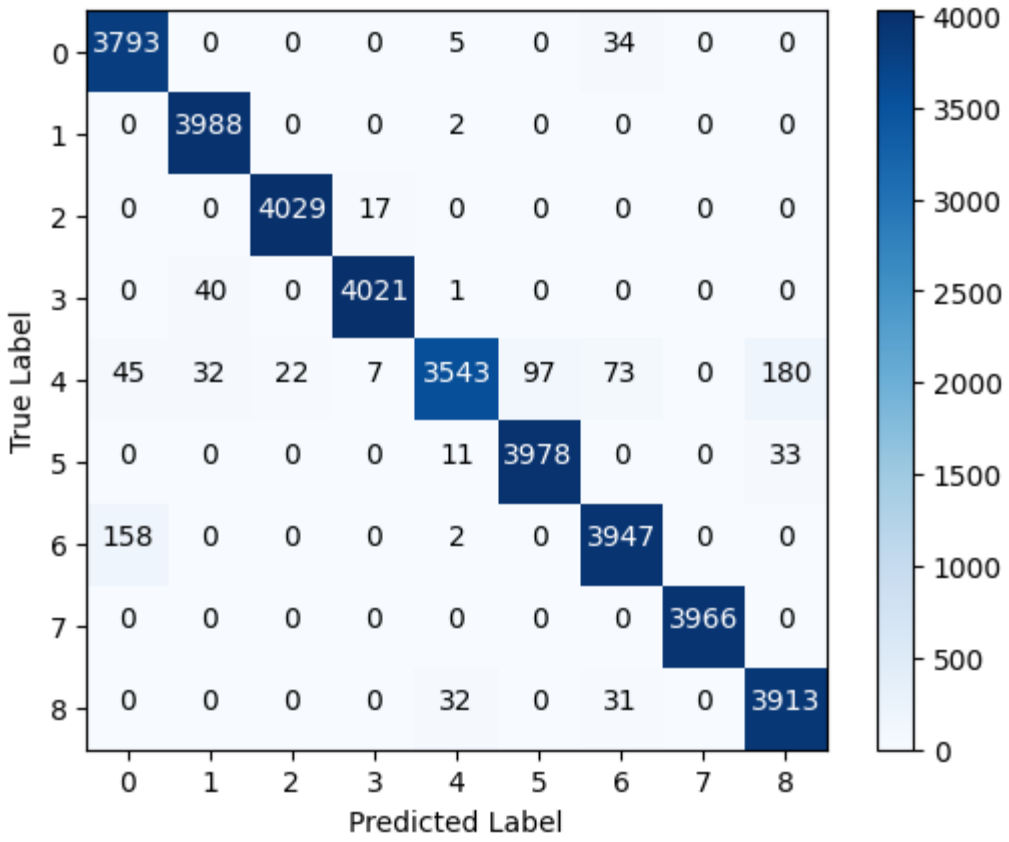

Figure 4 Confusion matrix LSTM-GRU

Although the hybrid model performed best compared to other associated models integrating CNN and LSTM-GRU architectures, this performance was intuitive because of its unified approach dealing with both spatial and temporal domains. Indeed, this had the highest aggregate accuracy (99%), precision (99%), recall(00%) and F1 score(98.95) of all tested models.

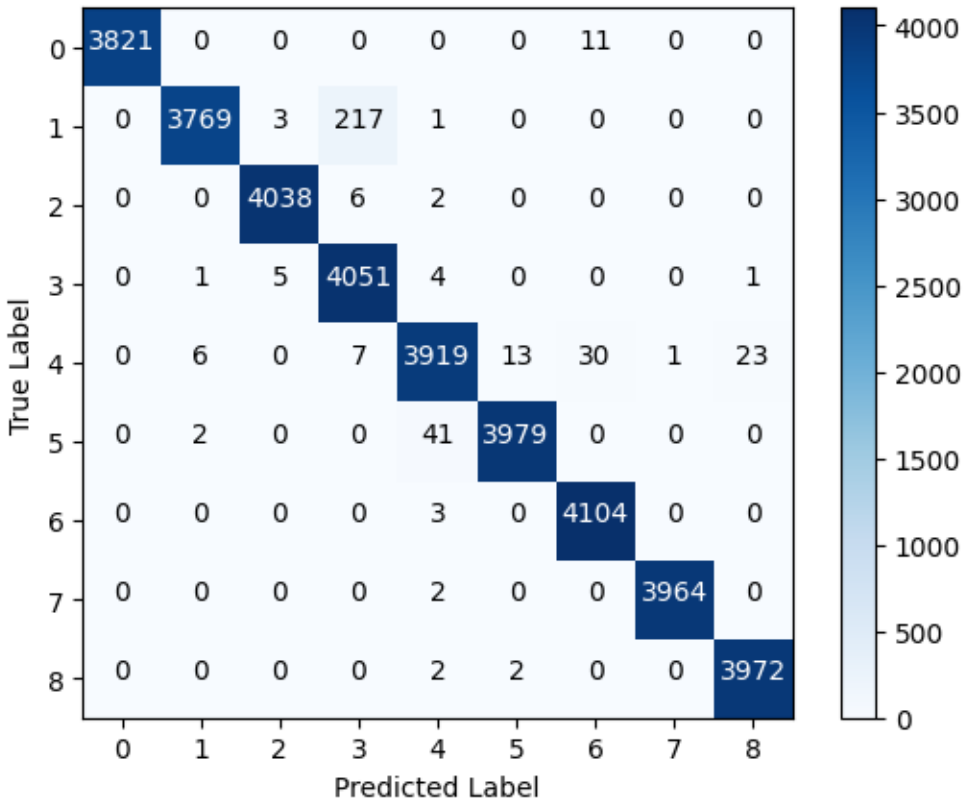

Figure 5 Confusion Matrix CNN-LSTM-GRU

11. Confusion Matrix Analysis

Based on the classification results of various types of network attack, further comparison from confusion matrices is shown for these models [40],[41],[42]. The matrices show good true positive rate in the most classes and as far mis-classifications are concerned, the hybrid model shows lowest value which continues to prove its better overall performance.

12. Comprehensive Analysis

Comparison across models performance in various metrics using bar chart shows that as the CNN, LSTM-GRU and Hybrid model all has similar results on their Key metrices; Accuracy, Precision, Recall and F1 score. The high level of uniformity indicates that each model excels within its domain—CNN with spatial features, LSTM-GRU with temporal and Hybrid works in the middle ground combining both.

This equal performance can be explained by the fact that this dataset is large and diverse, ensuring each model has a collection of examples allowing it to learn required patterns for obtaining high accuracy. This means the data itself lends well to different types of analysis (spatial, temporal, spatio-temporal).

Such findings are indispensable as they highlight that AI-based models can indeed improve the performance of traditional security devices, especially for complex IoT systems considering their huge diversities and data sizes providing a key point for the implementation of powerful yet efficient detection approaches. This could also indicate, as a rule of thumb for when computational efficiency is sought by design simpler models such as CNN or even LSTM-GRU would be able to perform similarly well yet giving us prediction capability. Nonetheless, the Hybrid model enables a strong suit for those cases in which one believes that combining spatial and temporal analysis could be advantageous.

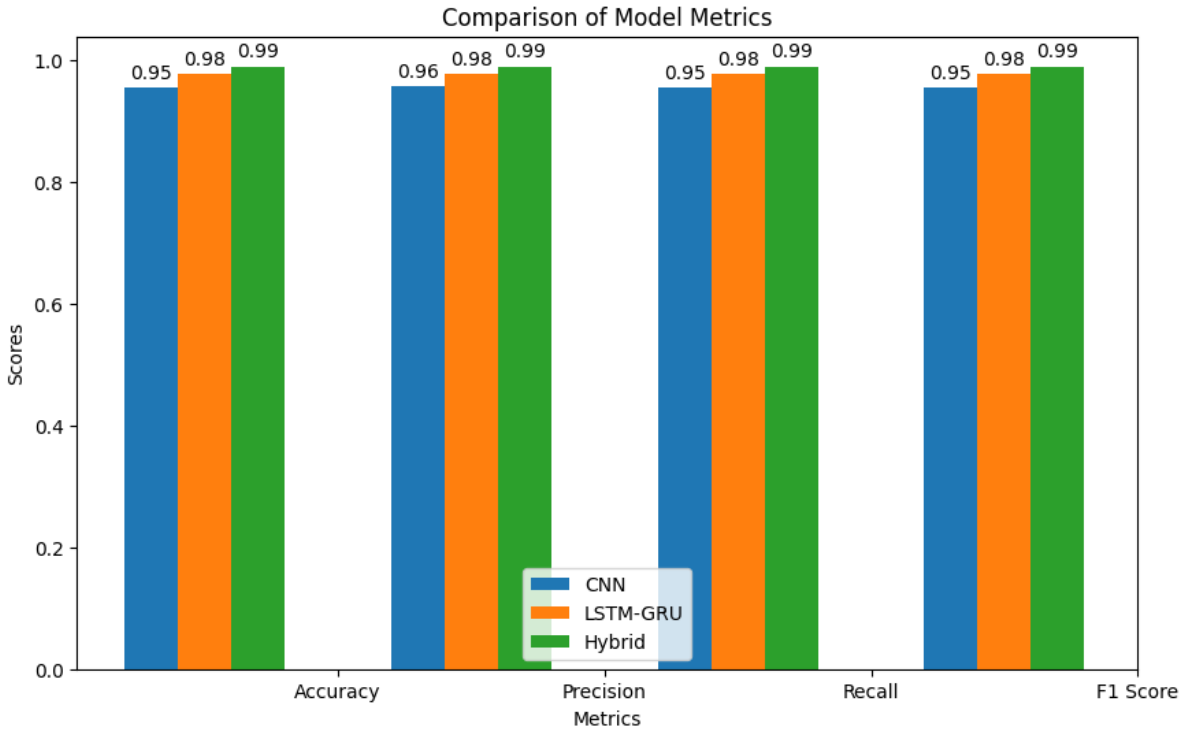

Figure 6 Comparison of Models Metrics

These results are essential for building efficient security tools such that the data diversity and volume of these environments make traditional intrusion detection mechanisms not optimally working in an IoT network. This high performance on the combined model means a useful avenue for research and retrieval in setting where speed is most important.

13. Conclusion

The study systematically explores and evidences the applicability of deep learning models for intrusion detection in IoT networks such that it helps security professionals to evolve measures required inside those intricate settings. The research produced stark advantages of using contemporary modelling techniques for anomaly detection in utilising a dataset relatively well-balanced between different classes - i.e. across various types of network intrusions and normal activities alike.

The specific problem resulted in the development and testing of three unique models by experimentations:CNN Model, LSTM-GRU Model and Hybrid model (combination on CNN + LSTM -GRUs) Especially, the hybrid model provided perfect 99% of Accuracy(), Precision(), Recall() and F1(). The reliability of this model in accommodating spatial and temporal features make it a strong candidate for easy implementation as security systems are concerned, towards IoT networks.

Performance metrics and confusion matrices also supported the isolated abilities of each model, as well as their complementarity when incorporated into a hybrid system (for better/unsatisfactorily suited comparison). This shows its power in providing a substantially lower false positive and negative rates as these can be major shortcomings of traditional intrusion detection systems.

A comparative analysis of the different performance metrics across the models was also provided, demonstrating that specific benefits arise from integrating multiple deep learning architectures. The aforementioned integrated approach increases the effectiveness of detection mechanisms and resilience to evolving, elaborate cyber threats.

The results of this study can provide a valuable guideline for future research related to cybersecurity, especially in the IoT context. Future work could involve practice; The scalability of the hybrid model needs to be evaluated in a

more robust and realistic manner, large network conditions as well assessing e performance up against real-time solutions such as intrusion detection. Also, if the models are going to continually be refined, they could include more detailed behavior data or new deep learning techniques that would focus even closer on idiosyncratic patterns of network anomalies.

This research not only takes a further step towards theoretical understanding of machine learning in cybersecurity, it also lays the groundwork for creating powerful and accurate intrusion detection systems that are vital to securing this ever-expanding digital domain filled by IoT networks.

14. References

1. Atadoga, A., Umoga, U. J., Lottu, O. A., & Sodiya, E. O. (2024). Evaluating the impact of cloud computing on accounting firms: A review of efficiency, scalability, and data security. Global Journal of Engineering and Technology Advances, 18(2), 065-074.
2. Rehan, H. (2024). Revolutionizing America's Cloud Computing the Pivotal Role of AI in Driving Innovation and Security. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 2(1), 239-240.
3. Darwish, D. (Ed.). (2024). Emerging Trends in Cloud Computing Analytics, Scalability, and Service Models.
4. Obi, O. C., Dawodu, S. O., Daraojimba, A. I., Onwusinkwue, S., Akagha, O. V., & Ahmad, I. A. I. (2024). Review of evolving cloud computing paradigms: security, efficiency, and innovations. Computer Science & IT Research Journal, 5(2), 270-292.
5. Heidari, A., & Jabraeil Jamali, M. A. (2023). Internet of Things intrusion detection systems: a comprehensive review and future directions. Cluster Computing, 26(6), 3753-3780.
6. Chang, V., Golightly, L., Modesti, P., Xu, Q. A., Doan, L. M. T., Hall, K., ... & Kobusińska, A. (2022). A survey on intrusion detection systems for fog and cloud computing. Future Internet, 14(3), 89.
7. Li, Z., Liu, F., Yang, W., Peng, S., & Zhou, J. (2021). A survey of convolutional neural networks: analysis, applications, and prospects. IEEE transactions on neural networks and learning systems, 33(12), 6999-7019.
8. A. Mishra and P. Yadav, “Anomaly-based IDS to detect attack using various artificial intelligence machine learning algorithms: a review,” in Proceedings of the 2nd International Conference on Data, Engineering and Applications, IDEA, Bhopal, India, February 2020.
9. K. Atefi, S. Yahya, A. Rezaei, and S. H. M. H. Binti, “Anomaly detection based on profile signature in network using machine learning technique,” in Proceedings of the 2016 IEEE Region 10 Symposium (TENSYMP), pp. 71–76, Sanur, Bali island, Indonesia, May 2016.
10. T. T. Khoei, G. Aissou, W. C. Hu, and N. Kaabouch, “Ensemble learning methods for anomaly intrusion detection system in smart grid,” in Proceedings of the 2021 IEEE International Conference on Electro Information Technology (EIT), pp. 129–135, Mt. Pleasant, MI, USA, May 2021.
11. T. Rakshe and V. Gonjari, “Anomaly based network intrusion detection using machine learning techniques,” International Journal of Engineering Research and Technology, vol. 6, no. 5, pp. 216–220, 2017.
12. V. Kumar, V. Choudhary, V. Sahrawat, and V. Kumar, “Detecting intrusions and attacks in the network traffic using anomaly-based techniques,” in Proceedings of the 2020 5th International Conference on Communication and Electronics
13. Z. Zhang, P. Chirupphapa, H. Esaki, and H. Ochiai, “XGBoosted misuse detection in LAN-internal traffic dataset,” in Proceedings of the 2020 IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 1–6, Arlington, VA, USA, November 2020.
14. K. A. Taher, B. Mohammed Yasin Jisan, and M. M. Rahman, “Network intrusion detection using supervised machine learning technique with feature selection,” in Proceedings of the 2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), pp. 643–646, Dhaka, Bangladesh, January 2019.
15. Y. Ye, L. Chen, S. Hou, W. Hardy, and X. Li, "DeepAM: a heterogeneous deep learning framework forcintelligent malware detection," Knowledge and Information Systems, vol. 54, no. 2, pp. 265-285, 2018. doi: 10.1007/s10115-017-1125-5.
16. Xianwei Gao et al., "Malware classification for the cloud via semi-supervised transfer learning," Journal of Information Security and Applications, vol. 55, p.102661-, 2020, doi: 10.1016/j.jisa.2020.102661.
17. M.Venkata Rao et al., "Deep Learning CNN Framework for Detection and Classification of Internet Worms," Journal of Interconnection Networks, vol .21, no .4, p .2144024-,2022.
18. H.Alkahtani and T.Aldhyani,"Artificial Intelligence Algorithms for Malware Detection in AndroidOperated Mobile Devices," Sensors (Basel Switzerland), vol .22 , no .6 , p .2268-,2022 ,doi:1.3390/s22062268.

19. Aboubakar, M., Kellil, M., & Roux, P. (2022). A review of IoT network management: Current status and perspectives. Journal of King Saud University-Computer and Information Sciences, 34(7), 4163-4176.
20. Hussain, F., Hassan, S. A., Hussain, R., & Hossain, E. (2020). Machine learning for resource management in cellular and IoT networks: Potentials, current solutions, and open challenges. IEEE communications surveys & tutorials, 22(2), 1251-1275.
21. Soares, K., & Shinde, A. A. (2024, March). Intrusion Detection Systems in VANET: A Review on Implementation Techniques and Datasets. In 2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) (pp. 897-905). IEEE.
22. Campos, E. M., Saura, P. F., González-Vidal, A., Hernández-Ramos, J. L., Bernabe, J. B., Baldini, G., & Skarmeta, A. (2022). Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges. Computer Networks, 203, 108661.
23. Kadiyala, A., & Kumar, A. (2017). Applications of Python to evaluate environmental data science problems. Environmental Progress & Sustainable Energy, 36(6), 1580-1586.
24. Bloice, M. D., & Holzinger, A. (2016). A tutorial on machine learning and data science tools with python. Machine Learning for Health Informatics: State-of-the-Art and Future Challenges, 435-480.
25. Castro, O., Bruneau, P., Sottet, J. S., & Torregrossa, D. (2023). Landscape of High-Performance Python to Develop Data Science and Machine Learning Applications. ACM Computing Surveys, 56(3), 1-30.
26. Priyambudi, Z. S., & Nugroho, Y. S. (2024, January). Which algorithm is better? An implementation of normalization to predict student performance. In AIP Conference Proceedings (Vol. 2926, No. 1). AIP Publishing.
27. Shakir, V., & Mohsin, A. (2024). A Comparative Analysis of Intrusion Detection Systems: Leveraging Algorithm Classifications and Feature Selection Techniques. Journal of Applied Science and Technology Trends, 5(01), 34-45.
28. Irie, K., Tüske, Z., Alkhouli, T., Schlüter, R., & Ney, H. (2016, September). LSTM, GRU, highway and a bit of attention: An empirical overview for language modeling in speech recognition. In Interspeech (pp. 3519-3523).
29. Shiri, F. M., Perumal, T., Mustapha, N., & Mohamed, R. (2023). A comprehensive overview and comparative analysis on deep learning models: CNN, RNN, LSTM, GRU. arXiv preprint arXiv:2305.17473.
30. Nosouhian, S., Nosouhian, F., & Khoshouei, A. K. (2021). A review of recurrent neural network architecture for sequence learning: Comparison between LSTM and GRU.
31. Haji, S. H., & Abdulazeez, A. M. (2021). Comparison of optimization techniques based on gradient descent algorithm: A review. PalArch's Journal of Archaeology of Egypt/Egyptology, 18(4), 2715-2743.
32. Wang, Q., Ma, Y., Zhao, K., & Tian, Y. (2020). A comprehensive survey of loss functions in machine learning. Annals of Data Science, 1-26.
33. Tian, Y., Su, D., Lauria, S., & Liu, X. (2022). Recent advances on loss functions in deep learning for computer vision. Neurocomputing, 497, 129-158.
34. Bhatt, C., Kumar, I., Vijayakumar, V., Singh, K. U., & Kumar, A. (2021). The state of the art of deep learning models in medical science and their challenges. Multimedia Systems, 27(4), 599-613.
35. ElRafey, A., & Wojtusiak, J. (2017). Recent advances in scaling-down sampling methods in machine learning. Wiley Interdisciplinary Reviews: Computational Statistics, 9(6), e1414.
36. Spagnolo, F., Gobbi, S., Zsoldos, E., Edde, M., Weigel, M., Granziera, C., ... & Magon, S. (2024). Down-sampling in diffusion MRI: a bundle-specific DTI and NODDI study. Frontiers in Neuroimaging, 3, 1359589.
37. Akhtar, N., & Ragavendran, U. (2020). Interpretation of intelligence in CNN-pooling processes: a methodological survey. Neural computing and applications, 32(3), 879-898.
38. Xie, Q., Viswanatha, S. K., Jayaram, S., Krishnankutty, S., Huguennet, F., Soni, R., & Basu, A. (2024, May). Effective Downsampling Techniques for SEM Defect Inspection Using Design Insights in Machine Learning: Topic/category: DI: Defect Inspection and Reduction. In 2024 35th Annual SEMI Advanced Semiconductor Manufacturing Conference (ASMC) (pp. 1-4). IEEE.
39. Ntlangu, M. B., & Baghai-Wadji, A. (2017, December). Modelling network traffic using time series analysis: A review. In Proceedings of the International Conference on Big Data and Internet of Thing (pp. 209-215).
40. Hoque, N., Bhuyan, M. H., Baishya, R. C., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network attacks: Taxonomy, tools and systems. Journal of Network and Computer Applications, 40, 307-324.
41. Aljabri, M., Aljameel, S. S., Mohammad, R. M. A., Almotiri, S. H., Mirza, S., Anis, F. M., ... & Altamimi, H. S. (2021). Intelligent techniques for detecting network attacks: review and research directions. Sensors, 21(21), 7070.
42. Ahmetoglu, H., & Das, R. (2022). A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions. Internet of Things, 20, 100615.

حلول الأمن السحابية المبتكرة: نماذج RNN الهجينة ونماذج CNN للكشف عن التسلل

احمد أكبر محمد
جامعة ازاد ، كلية هندسة الحاسبات، قسم البرمجيات، جنوب طهران،ايران.
kahmed833@gmail.com

الخلاصة: لقد انتقلت البنى التحتية للحوسبة السحابية إلى قلب العمليات التجارية العالمية، مما يضعها أيضاً في موقع رئيسي للعديد من التحديات الإلكترونية المتقدمة التي تواجهها. وهذا يجعل أنظمة كشف التسلل التقليدية القائمة على القواعد المحددة مسبقاً والمعروفة والقائمة على التوقيعات (IDS) عديمة الفائدة تقريباً في هذا العصر من التهديدات المتقدمة، بما في ذلك هجمات اليوم الصفري والتهديدات المستمرة المتقدمة APTs – التهديدات المستمرة المتقدمة التي تستغل البرمجيات الخبيثة متعددة الأشكال. تقدم هذه الورقة البحثية نموذجًا ثوريًا هجينًا يستخدم قوة الشبكات العصبية المتكررة (RNN) والشبكات العصبية التلافيفية (CNN) لتطوير نظام كشف التسلل القائم على السحابة. وتستخدم هذه الطريقة الهجينة شبكة الشبكات العصبية المتكررة (RNN) للتشفير والتعلم من بيانات السلاسل الزمنية، واكتساب ذاكرة على الشذوذ الزمني في المعلومات؛ بالإضافة إلى ذلك، تستخدم هذه الطريقة الهجينة الشبكات العصبية التلافيفية بشكل مكثف لاستخراج السمات المكانية بإنتاجية عالية والتي تصبح ضرورية للكشف عن هذه الأنماط عبر العديد من الأنماط التي تشير إلى حدوث اختراقات. في بيئة سحابية واضحة المعالم، نقوم بتقييم الفعالية الإجمالية لهذا النموذج من خلال اختباره في ظل العديد من سيناريوهات الهجوم. تشير نتائجنا إلى أن هذا النموذج لا يتفوق فقط على أنظمة تحديد الهوية القياسية من حيث الكشف عن الهجمات الإلكترونية فحسب، بل يُظهر أيضًا مرونة فائقة ضد تهديدات اليوم الصفر والتهديدات الناشئة. من الواضح أن هذه الكفاءة المتزايدة في الكشف ضرورية لضمان أمن وموثوقية الخدمات السحابية، مما يسمح بآليات دفاعية أكثر صرامة والتي تظل ضرورية في بيئة التهديدات الإلكترونية الحديثة المتطورة ديناميكيًا.

الكلمات المفتاحية: أمن السحابة، أنظمة كشف التسلل، التعلم العميق، الشبكات العصبية المتكررة، الشبكات العصبية التلافيفية، كشف التهديدات السيبرانية.