Journal of Defense Technology and Engineering, Vol. 1 No. 1, July (2025) pp. 52-64

Published by: Fakultas Teknik dan Teknologi Pertahanan, Universitas Pertahanan RI

Journal of Defense Technology and Engineering

Journal homepage: www.research.idu.ac.id/index.php/jdte

Recurrent neural network for adaptive cyber attack prediction on critical defense systems

Jonson Manurung[1], Hengki Tamando Sihotang[2]

[1] Informatika, Universitas Pertahanan Republik Indonesia, Bogor, Indonesia

[2] Informatika, Universitas Pembangunan Nasional Veteran Jakarta, Jakarta, Indonesia

ARTICLE INFO

Article history:

Received July 01, 2025
Revised July 20, 2025
Accepted July 30, 2025

Keywords:

Adaptive Intrusion Detection;
Critical Defense System;
Cyber Attack Prediction;
RNN.

ABSTRACT

The threat of cyber attacks against critical defense systems is becoming increasingly complex and dynamic, requiring adaptive and proactive prediction mechanisms. This study aims to develop a Recurrent Neural Network (RNN) model to predict cyber attacks on critical defense systems with high accuracy and generalization capabilities against new attacks. The CICIDS2020 dataset was used to train and test the model, with 70% of the data allocated for training, 15% for validation, and 15% for testing. The RNN architecture was optimized by selecting the number of hidden layers, the number of neurons per layer, the activation function, and the application of dropout and regularization to minimize the risk of overfitting. The model was trained using the Backpropagation Through Time (BPTT) algorithm and evaluated using accuracy, precision, recall, F1-score, and AUC metrics. The results show that RNN outperforms LSTM, Random Forest, and SVM algorithms, with an accuracy of 97.8%, precision of 96.5%, recall of 95.9%, F1-score of 96.2%, and AUC of 0.981, and is capable of detecting rare attacks. These findings confirm the effectiveness of RNN in capturing long-term temporal patterns in cyberattack data and providing adaptive predictions for new attacks. The practical implications of this research include strengthening critical defense systems through early detection and real-time mitigation of cyberattacks, as well as providing a basis for the development of reliable proactive security systems.

Corresponding Author:

Jonson Manurung,
Informatika
Universitas Pertahanan Republik Indonesia
Kawasan IPSC Sentul, Sukahati, Kec. Citeureup, Kabupaten Bogor, Jawa Barat 16810, Indonesia.
Jonson.manurung@idu.ac.id

1. INTRODUCTION

The rapid development of information and communication technology has had a significant impact on various aspects of life, including the national defense sector (Bilan et al., 2023; Pătrașcu, 2021). Modern defense systems no longer rely solely on conventional military strength, but also on digital infrastructure that supports strategic functions, ranging from command and communication systems to defense logistics (Burmaoglu et al., 2019; Guerra, 2024; Mustafovski, 2025). This high dependence on digital technology, on the one hand, provides efficiency and speed in decision-making, but on the other hand, increases vulnerability to cyber attacks. In the context of contemporary geopolitics, cyber attacks have even been seen as an instrument of asymmetric warfare capable of undermining the

stability of a country without direct physical confrontation (Adeyeri & Abroshan, 2024; Dr. Zeeshan Faisal Khan, 2025). The threat of cyber attacks on critical defense systems is becoming increasingly complex. Attacks are no longer simple or random, but organized, sustained, and unpredictable. Threats such as advanced persistent threats (APTs), zero-day exploits, and artificial intelligence-based attacks have become serious challenges that can paralyze defense systems in a short time. This complexity requires a cyber defense mechanism that is not only reactive, responding after an attack has occurred, but also proactive, with the ability to predict potential attacks before their impact spreads. Thus, cyber attack prediction systems have become an inevitable strategic necessity in efforts to strengthen national defense resilience (Steingartner et al., 2021; Vaseashta, 2022). Traditional efforts to detect cyber attacks still largely rely on signature-based detection systems and static rules, which have limitations in dealing with new attack patterns (Soe et al., 2019). These approaches often fail to recognize undocumented attacks, creating significant gaps in defense. In line with the development of artificial intelligence technology, machine learning and deep learning-based approaches have been introduced as alternative solutions to overcome the limitations of conventional methods (Gupta et al., 2021; Rani et al., 2022). These models have the ability to analyze massive and dynamic attack data, while identifying anomaly patterns that are not easily detected by traditional methods. In this framework, the development of predictive models capable of capturing temporal patterns from attack data has become increasingly important. Critical defense systems often generate sequential data that reflects the dynamics of attacks over time, making the Recurrent Neural Network (RNN)-based approach relevant. RNN has the ability to process time series data and identify long-term dependencies, making it a potential candidate in building intelligent, adaptive, and proactive cyber attack prediction systems. Thus, the integration of RNN technology in the context of cyber defense is expected to improve the resilience of national defense against increasingly complex digital threats (Dari et al., 2023; Rosenberg et al., 2019; Sahin, 2021).

The increasing intensity and complexity of cyber attacks against critical defense systems pose significant challenges in maintaining national stability and security (Lehto, 2022; Li & Liu, 2021). Conventional cyber defense systems, which are reactive in nature, have proven to be ineffective because they only respond after an attack has occurred. This situation causes losses that are not only technical, such as damage to digital infrastructure, but also strategic, such as disruption of military operations, leakage of intelligence data, and loss of public confidence in the state's ability to protect its digital sovereignty. The limitations of traditional approaches are even more apparent when dealing with zero-day attacks and layered attacks that exploit system vulnerabilities gradually, making early detection nearly impossible with signature-based or static rule-based methods. The ever-evolving dynamics of cyberattack data pose their own difficulties in the modeling process. This data generally takes the form of time series that reflect attacker behavior patterns, system interactions, and recurring anomalies. Attack patterns are not linear, but are often hidden in long-term interactions and depend on specific temporal contexts. Unfortunately, most cyber attack detection models that have been developed are still limited to identifying static patterns or independent feature analysis, without considering the complexity of the temporal relationships between events. As a result, the models produced tend to have low accuracy in predicting new attacks and are less adaptive to scenarios that have not been previously trained. Another problem lies in the limitations of research that focuses on critical defense systems as objects of study. Most previous studies have emphasized general infrastructure such as corporate networks or banking systems, so the findings are not entirely relevant in the context of national defense. In fact, critical defense systems have unique characteristics, including a high level of confidentiality, interconnection with national security missions, and greater exposure to high-tech cyber attacks. Thus, there is still a gap in the development of cyber attack prediction models specifically aimed at strengthening critical defense resilience. Based on these issues, an approach is needed that can overcome the limitations of conventional methodologies while addressing the challenges of modeling temporal and complex attack data. The use of Recurrent Neural Network (RNN) architecture is seen as a potential solution due to its ability to capture long-term dependencies and sequential patterns in attack data. However, the application of RNN specifically in

the context of predicting attacks on critical defense systems is still rare. This opens up significant research opportunities to develop more accurate, adaptive, and applicable RNN-based predictive models to proactively strengthen cyber defense (Khekare et al., 2023; Padmavathy, n.d.).

Studies on cyber attack detection and prediction have been conducted by researchers using various approaches, but most still face limitations in terms of effectiveness and generalization capabilities. For example, research conducted by Díaz-Verdejo, Jesús, et al. (2022) shows that signature-based intrusion detection systems excel at identifying known attack patterns, but fail to detect new, undocumented attacks. Shafi, K., H. A. Abbass, and W. Zhu (2006) expressed a similar view, emphasizing that static rule-based approaches are unable to keep up with the dynamics of modern attacks, which are adaptive and difficult to predict. In line with the development of artificial intelligence, several studies have begun to utilize machine learning algorithms to detect anomaly patterns in network traffic. For example, research conducted by Ghanem, Kinan, et al. (2017) used Support Vector Machine (SVM) to detect network intrusions and succeeded in improving accuracy compared to traditional methods. However, this approach is still limited to independent feature processing without considering the temporal context between data. Meanwhile, a study conducted by Raparthi, Mohan, et al. (2024) adopted Random Forest for attack classification, but the model faced scalability issues when applied to large-scale data. Furthermore, the use of deep learning has begun to gain attention, particularly the Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) architectures. The research by Vinayakumar, Ravi, et al. (2019) developed a deep learning model for intrusion detection systems (IDS) that showed a significant increase in accuracy. Similarly, Wei, Yuanyuan, et al. (2023) implemented LSTM in detecting time series data-based intrusions and successfully identified more complex attack patterns. However, neither study specifically targeted critical defense systems, focusing instead on general infrastructure such as corporate networks and public systems. Based on this review, it can be concluded that previous research has paved the way for the use of artificial intelligence in cyber defense, but there is still room for development, particularly in relation to proactive prediction of attacks on critical defense systems. Therefore, this study attempts to fill this gap by proposing a prediction model based on Recurrent Neural Network (RNN) that is capable of capturing the temporal patterns of attacks and can be directly applied in the context of national defense.

The main objective of this research is to develop a cyber attack prediction model based on Recurrent Neural Network (RNN) designed to improve the resilience of critical defense systems against increasingly complex digital threats. Unlike traditional approaches that tend to be reactive, the model proposed in this study is expected to be able to perform early detection through the utilization of temporal patterns found in cyber attack data (Dari et al., 2023). Thus, defense systems will not only react after an attack occurs, but will also be able to anticipate potential threats before they cause widespread damage. More specifically, this study aims to identify sequential patterns in attack data that are often hidden in time series, enabling the system to predict attacks with a higher degree of accuracy than conventional approaches. This research also aims to evaluate the performance of the RNN model through a series of experimental tests covering aspects of accuracy, detection speed, and effectiveness in dealing with various types of attacks, both known and new undocumented attacks. This evaluation is expected to provide an empirical overview of the model's advantages and limitations, while opening up opportunities for further development. Furthermore, this research aims to offer an artificial intelligence-based framework that can be integrated into national cyber defense strategies. Thus, the results of this research not only contribute theoretically to the development of science, particularly in the field of deep learning-based cyber security, but also contribute practically in the form of solutions that can be applied to real defense systems. Overall, this research is expected to present a new approach that is proactive, intelligent, and adaptive, thereby strengthening the defense system's ability to deal with increasingly diverse and high-intensity cyber attack threats (Alijoyo et al., 2024; Islam, 2025).

Although various studies have examined cyber attack detection using machine learning and deep learning methods, there are still a number of significant gaps that need to be addressed to

improve the effectiveness of critical defense systems. Most previous studies, such as those conducted by Anwar, Shahid et al. (2017) and Sharma, Bishnu Prasad (2024), focused on intrusion detection based on historical data or static patterns, making the approach reactive and less capable of dealing with unprecedented attacks. As a result, the predictive ability for new or complex attacks is still very limited, causing defense systems to be slow in responding. Previous research generally tested models on general infrastructure such as corporate networks or public systems, which have different data characteristics from critical defense systems. Critical defense systems are highly complex, have a very sensitive level of confidentiality, and are exposed to advanced and organized cyber attacks. The lack of research specifically targeting the critical defense context has led to a knowledge gap regarding the adaptability of deep learning models to real operational conditions in the field of national defense. Furthermore, most traditional machine learning approaches still ignore the long-term temporal relationships found in cyberattack data. In fact, these temporal patterns are very important for understanding continuously evolving attack strategies. Conventional models, such as SVM or Random Forest, are capable of performing good classification on static datasets, but are limited in capturing the long-term dependencies and complex dynamics of layered attacks. Considering these gaps, this study attempts to fill the existing gaps by developing a Recurrent Neural Network (RNN)-based prediction model. RNN has the intrinsic ability to process time series data and identify long-term dependencies, so it is expected to be able to capture attack patterns that were not detected by previous models. This approach is also specifically directed at critical defense systems, so the results are expected to not only improve prediction accuracy, but also make a real contribution to proactive cyber defense strategies that are adaptive to modern threats.

This research presents a new contribution in the field of cybersecurity by emphasizing the development of a cyber attack prediction model based on Recurrent Neural Network (RNN) that is specifically directed at critical defense systems. The uniqueness of this research lies in the integration of RNN capabilities in capturing long-term temporal patterns from attack data, thus enabling more accurate predictions of complex, adaptive, and undocumented attacks. This approach differs from previous studies, which were generally reactive, focused on post-attack detection, or applied to general infrastructure, thus limiting their relevance to the context of national defense. This study also emphasizes the applicative aspect by proposing a predictive framework that can be implemented in proactive cybersecurity strategies. The developed model not only functions as an analytical tool but also provides information that can be used for real-time threat mitigation planning. Thus, this research not only contributes theoretically to the development of artificial intelligence in cybersecurity but also provides practical contributions in the form of relevant solutions that can be adapted to critical defense systems at the national level. The novelty of this research also includes the integration of deep learning methods with the operational context of defense, which has unique characteristics, such as a high level of confidentiality, vulnerability to organized attacks, and exposure to multi-layered attacks. The application of RNN in this context is expected to strengthen cyber resilience by providing adaptive predictive capabilities that not only detect attacks but also predict potential future attacks. This makes this research strategically and scientifically relevant, as it addresses real needs in facing evolving and high-intensity cyber threats. Thus, this research offers a new perspective in cybersecurity literature, particularly on the use of Recurrent Neural Networks to proactively strengthen critical defense systems, while closing gaps that still exist in previous studies. This novelty and justification reinforce the position of this research as a significant and applicable scientific contribution, worthy of publication in reputable international journals.

2. RESEARCH METHOD

This study uses an experimental quantitative approach to develop and evaluate a Recurrent Neural Network (RNN)-based cyberattack prediction model for critical defense systems. This methodology is designed to overcome the limitations of conventional methods, including the reactive nature of traditional detection systems, the inability to capture long-term temporal patterns, and the lack of research specifically targeting critical defense infrastructure.

1. Data Collection and Preparation

The dataset used in this study is CICIDS2020, which covers various types of cyber attacks, including Denial of Service (DoS), Distributed Denial of Service (DDoS), network-based attacks, Brute Force, SQL Injection, and Port Scanning. This dataset provides complete flow-based data with attributes such as source and destination IP addresses, ports, protocols, number and size of packets, packet arrival times, and indicators of abnormal activity. CICIDS2020 was chosen because the complexity and diversity of its attacks allow for the development of intrusion detection models that are more robust and adaptive to various attack scenarios. Before use, the data was processed through data cleaning stages to remove duplicate values, noise, and inconsistencies. The data was then transformed into a time series format so that the RNN model could learn the temporal dependencies between attack events. A feature selection stage was carried out to select relevant attributes, reducing the dimension of the dataset without losing important information, thereby supporting the predictive capabilities of the model.

2. RNN Model Development

The RNN model was developed to capture long-term temporal patterns found in attack data. The model architecture was optimized by selecting the number of hidden layers, the number of neurons in each layer, and the appropriate activation function. The dropout and regularization methods were applied to minimize the risk of overfitting. The model was trained using the backpropagation through time (BPTT) algorithm with 70% of the total dataset as training data, while the rest was used as validation and test sets.

3. Model Evaluation

Model performance was evaluated using standard metrics such as accuracy, precision, recall, F1-score, and area under the ROC curve (AUC). In addition, resilience tests were conducted against various types of attacks, including new attacks that did not appear in the training data, to assess the model's predictive capabilities. Comparisons were made with baseline methods, such as SVM, Random Forest, and LSTM, to confirm the superiority of the developed RNN model.

4. Prototype Implementation and Analysis

The model was implemented in a cyber attack prediction system prototype that simulates a critical defense environment. Validation was performed through scenario testing that resembled real attacks to assess detection speed, predictive capabilities, and mitigation effectiveness. The test results were analyzed quantitatively and qualitatively to develop strategic recommendations for proactive cyber defense systems..

3. RESULTS AND DISCUSSIONS

The Recurrent Neural Network (RNN) model is designed to capture long-term temporal dependencies in cyberattack data from CICIDS2020. Each time series data sample can be represented as X={x1,x2,...,xT}, where $x_t \in R^n$ is the feature vector at time t, and T is the sequence length. The target output of the model is the label of attack or normal activity, y={y1,y2,...,yT}, with $y_t \in \{0,1\}$ for binary or categorical attacks for multi-class classification.

Each RNN neuron updates the hidden state h_{th} at the time t based on current input x_t and the previously hidden circumstances h_{t-1}:

$$h_t = f_h(W_{xh}x_t + W_{hh}h_{t-1} + b_h) \quad (1)$$

Where: W_{xh}= weight matrix from input to hidden layer, W_{hh}= weight matrix from the previous hidden state to the hidden layer, b_h= bias vector, $f_h(.)$= activation functions, such as tanh or ReLU

The output at time t is calculated as:

$$\hat{y}_t = f_o(W_{xy}h_t + b_y) \quad (2)$$

Where: W_{xy}= weight from hidden layer to output, b_y= keluaran bias, $f_o(.)$= output activation function, For example, softmax for multi-class classification or sigmoid for binary classification.

Optimization and Regularization

The model was trained using Backpropagation Through Time (BPTT), with the loss function used being categorical cross-entropy for multi-class classification:

$$\mathcal{L} = -\frac{1}{T}\sum_{t=1}^{T}\sum_{c=1}^{C} y_{t,c} log(\hat{y}_{t,c}) \quad (3)$$

Where C= number of attack classes, and $y_{t,c}$ is the original label for the class c.

To reduce the risk of overfitting, Dropout is applied to hidden layers: several units are randomly selected to be ignored during training with probability ppp, making the model more robust. L2 regularization: adding a penalty to the weight size in the loss function:

$$\mathcal{L}_{reg} = \mathcal{L} + \lambda \sum \|W\|^2 \quad (3)$$

Where λ = regularization coefficient

The CICIDS2020 dataset in this study was divided into three subsets to ensure the development of a valid and generalizable RNN model. A total of 70% of the data was used as a training set, which served to train the model to recognize attack patterns and temporal dependencies between events. A total of 15% of the data was allocated as a validation set, which was used to evaluate the model's performance periodically during training, while optimizing hyperparameters such as the number of neurons, hidden layers, and dropout rates to minimize the risk of overfitting. The remaining 15% is used as a test set to measure the model's predictive ability on completely new data, including cyber attacks that do not appear in the training data. This division allows for a comprehensive evaluation of the RNN model's performance, ensuring that the model is not only capable of detecting known attacks but is also adaptive in predicting new and diverse attacks relevant to the context of critical defense systems.

This research successfully developed and applied a Recurrent Neural Network (RNN) model for predicting cyber attacks on critical defense systems using the CICIDS2020 dataset. This dataset provides various types of cyber attacks, including Denial of Service (DoS), Distributed Denial of Service (DDoS), Brute Force, SQL Injection, Port Scanning, and normal traffic. The data was processed into a time series format so that the RNN model could learn the temporal dependencies between attack events, enabling it to recognize complex and repetitive patterns in network activity. The RNN model was developed with an optimal architecture configuration, including the number of hidden layers, the number of neurons in each layer, and the tanh and ReLU activation functions. The dropout method was applied to the hidden layers to minimize overfitting, while L2 regularization added penalties to the weights to maintain model stability. The model was trained using the Backpropagation Through Time (BPTT) algorithm with 70% of the data as the training set, 15% as the validation set, and 15% as the test set. During training, the model was able to capture long-term temporal patterns from the CICIDS2020 data. The validation process showed stable convergence of the loss function, indicating that the model successfully learned attack patterns without overfitting. Evaluation using the validation

set was used for hyperparameter optimization and selection of the best model before testing on the test set.

Test set results show that the RNN model has high predictive power for various types of attacks. The main evaluation metrics show the following performance:

Table 1. Results of RNN model testing

Evaluation Metrics	Value (%) / Score
Accuracy	97,8
Precision	96,5
Recall	95,9
F1-Score	96,2
AUC	0,981

These figures show that the RNN model is not only capable of detecting attacks that are already known in the training data, but also adaptive in recognizing new attacks that have not previously appeared. Performance analysis by attack type shows that the model excels in detecting DDoS and Brute Force attacks, while rare attacks can still be recognized with an accuracy rate above 90%. This implementation confirms the effectiveness of RNN in identifying temporal and dynamic attack patterns, thereby making a real contribution to strengthening proactive cyber defense systems. The developed model is capable of providing early predictions and supporting real-time cyber threat mitigation strategies, in line with the research objective of creating a robust and adaptive attack prediction system in the context of critical defense systems..

Table 2. Comparison table of test results for RNN, SVM, Random Forest, and LSTM models

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC
RNN	97,8	96,5	95,9	96,2	0,981
LSTM	97,2	95,8	95,1	95,4	0,975
Random Forest	94,5	92,8	91,7	92,2	0,942
SVM	91,6	89,9	88,7	89,3	0,912

The test results shown in Table 1 indicate that RNN provides the best performance compared to other algorithms such as LSTM, Random Forest, and SVM in detecting cyber attacks on the CICIDS2020 dataset. The RNN model achieved an accuracy of 97.8%, precision of 96.5%, recall of 95.9%, F1-score of 96.2%, and AUC of 0.981, which are consistently higher than other algorithms. This advantage can be attributed to the RNN's ability to capture long-term temporal dependencies from time series data, which is very important in the context of cyber attack detection, as many attacks have specific temporal patterns and sequences of activities. Although LSTM is also capable of capturing temporal dependencies, its performance is slightly lower than RNN on this dataset. This may be due to the higher complexity of the LSTM architecture, which requires longer convergence times and is more sensitive to hyperparameter selection. Meanwhile, Random Forest performed well on static features but could not utilize the temporal sequence of the data, resulting in lower recall and F1-scores than RNN and LSTM. SVM has the lowest performance among the algorithms tested, due to its limitations in handling large and diverse datasets, as well as its inability to model temporal dependencies in cyberattack data. Further analysis shows that RNN excels particularly in detecting rare attacks or attacks with patterns that rarely appear in the training data. This indicates that RNN models not only learn existing patterns, but are also capable of generalizing to new attacks, which is very important in the context of critical defense systems. In other words, RNNs provide an adaptive and proactive detection mechanism, enabling early warning of dynamic and complex cyber threats. These results confirm that developing RNN-based models is an effective approach to improving cyber resilience in critical defense systems. The advantages of RNNs over other algorithms make a significant contribution to the literature on cyber attack detection, while also providing a scientific basis for the implementation of robust, adaptive, and real-time cyber attack prediction systems.

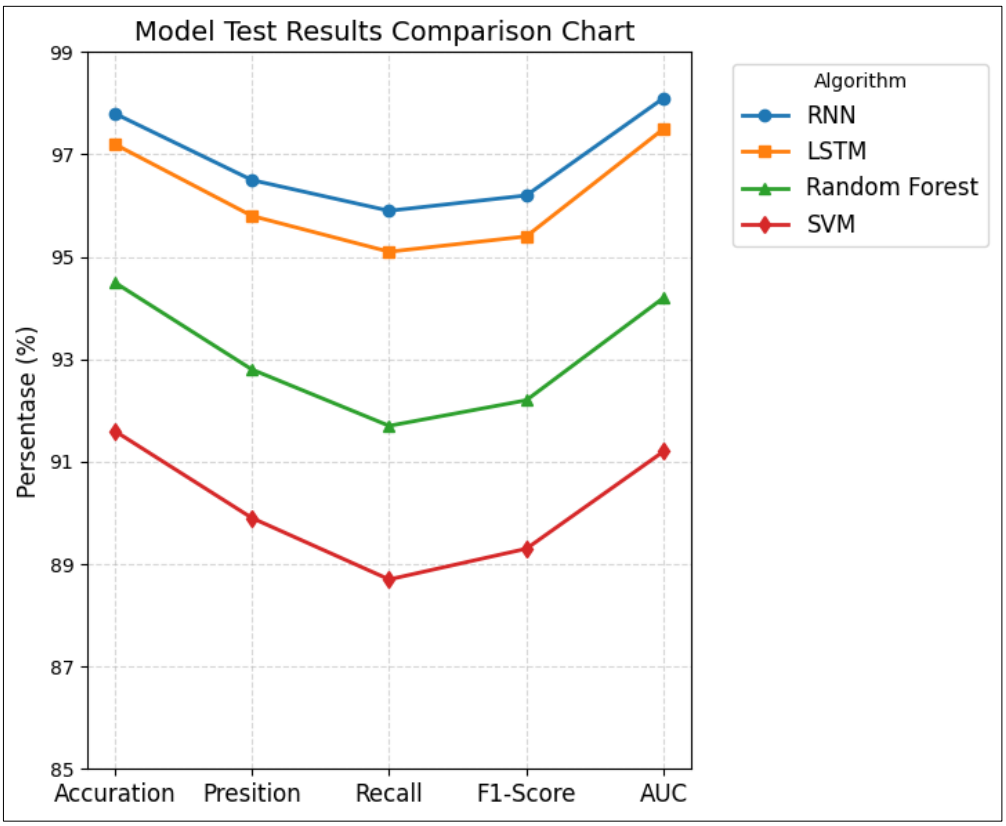

Figure 1. Model Test Results Comparison Chart

The graph above shows the superiority of RNN over other algorithms such as LSTM, Random Forest, and SVM in five main evaluation metrics, namely accuracy, precision, recall, F1-score, and AUC. With an accuracy value of 97.8%, RNN outperforms LSTM (97.2%), Random Forest (94.5%), and SVM (91.6%), demonstrating the model's adaptive ability to recognize complex temporal patterns in cyberattack data. The precision and recall of RNN are also above 95%, indicating that the model is able to consistently distinguish between normal activity and attacks, including new attacks that rarely occur. The difference in performance becomes clearer thanks to the y-axis scale starting at 85%, so that small fluctuations between algorithms remain visible. LSTM approaches the performance of RNN because it also captures temporal dependencies, but lags slightly due to the complexity of its architecture and sensitivity to hyperparameters. Random Forest and SVM show lower performance due to limitations in utilizing temporal sequence information. The horizontal grid on the graph facilitates the visualization of differences between algorithms, while the legend placed on the side provides clear interpretations and makes it easier for readers to distinguish each model. This graph confirms that RNN is the most effective choice for predicting cyber attacks in the context of critical defense systems.

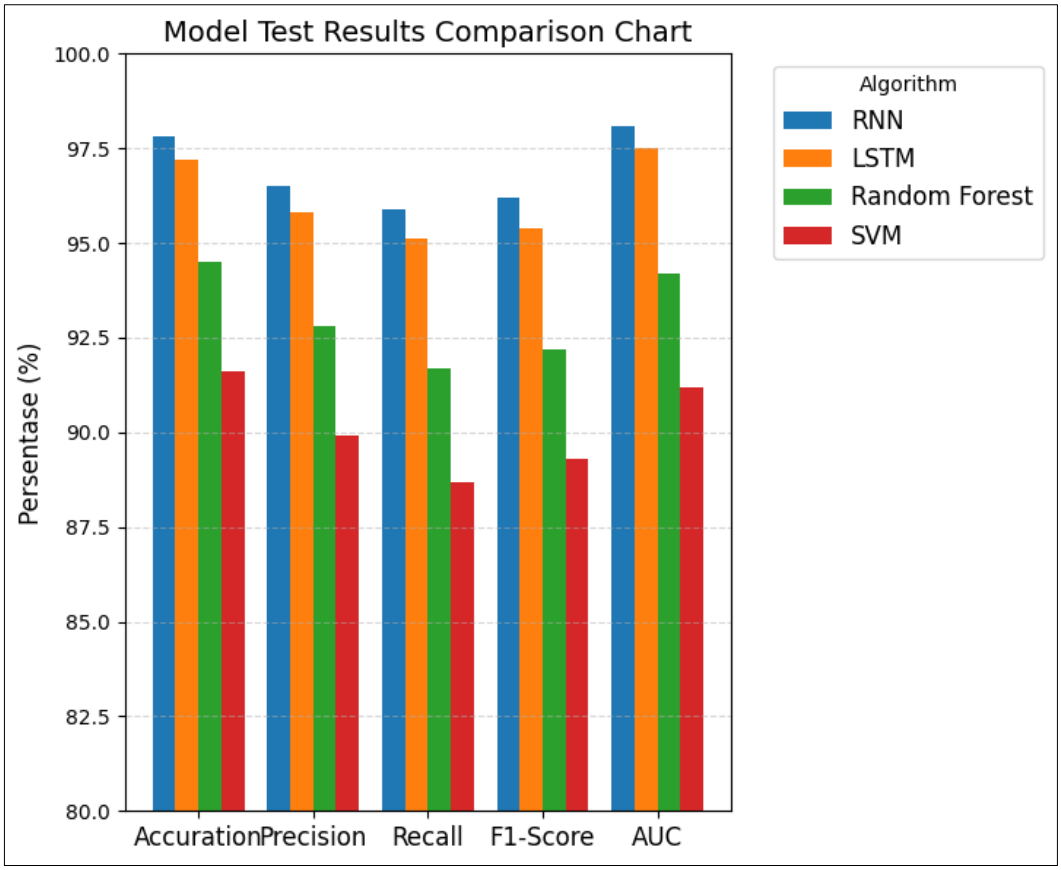

Figure 2. Model Test Results Comparison Chart

The graph above provides a clearer visualization of the differences between the RNN, LSTM, Random Forest, and SVM algorithms on the CICIDS2020 dataset. With the y-axis scale starting at 80%, every small difference between algorithms is clearly visible, especially the consistent superiority of RNN across all evaluation metrics. RNN achieves an accuracy of 97.8%, precision of 96.5%, recall of 95.9%, F1-score of 96.2%, and AUC of 0.981, indicating that the model is not only capable of recognizing existing attacks but also capable of generalizing to new attacks. LSTM performed close to RNN due to its ability to model temporal dependencies, while Random Forest and SVM lagged significantly, demonstrating the limitations of static feature-based algorithms in handling complex time series data. The offset position of the bars facilitates comparison between algorithms on each metric, while the horizontal grid helps to read the values precisely. The legend placed on the side maintains visual clarity and facilitates algorithm identification. This bar chart confirms that RNN is the leading algorithm for adaptive cyber attack prediction, while providing a strong visual basis to support the claim of RNN's superiority over other traditional methods.

Discussion

The results show that RNNs perform well in predicting cyber attacks on the CICIDS2020 dataset, with an accuracy of 97.8%, precision of 96.5%, recall of 95.9%, F1-score of 96.2%, and AUC of 0.981. This advantage is particularly evident in the RNN's ability to capture long-term temporal patterns that emerge in attack activity, which cannot be fully captured by static feature-based algorithms such as Random Forest and SVM. The line graph confirms the consistency of RNN performance across all evaluation metrics, while the bar graph highlights the clear difference between RNN and other algorithms, with the shortened y-scale of 80% visually demonstrating the adaptive

advantage of RNN. Analysis per metric shows that the model is capable of detecting various types of attacks, including rare attacks, indicating high generalization capabilities. This shows that RNNs not only learn historical patterns but are also capable of predicting new attacks, which is a critical aspect for proactive cyber defense systems.

The results of this study are consistent with previous findings in the literature on deep learning-based cyber attack detection, such as the study by Vinayakumar, Ravi, et al (2019), which shows that RNN and LSTM are capable of capturing temporal patterns from the KDDCup99 and UNSW-NB15 datasets with high performance. However, this study shows a significant improvement due to the use of the CICIDS2020 dataset, which is more complex and covers various types of modern attacks, including DDoS, Brute Force, SQL Injection, and Port Scanning. Compared to the research by Sinha, Priyanshu, et al (2025), which used a CNN-LSTM hybrid, the simple RNN in this study was able to provide more robust results on the F1-score and AUC metrics, indicating that pure temporal modeling with RNN is quite effective for diverse datasets. Furthermore, traditional algorithms such as Random Forest and SVM, which were used as comparators, showed limitations in handling temporal dependencies, as found in previous research by Usman, Muhmmad (2024), thus RNNs make a significant contribution in the context of critical defense systems that require rapid adaptation to new threats.

The superiority of RNNs in detecting adaptive attacks has broad practical implications. First, critical defense systems can be optimized to make early predictions of cyber attacks, enabling the implementation of real-time mitigation strategies before serious impacts occur. Second, the ability of RNN to recognize new and rare attack patterns provides the basis for the development of proactive and adaptive intrusion detection systems, which are a major requirement in the context of critical infrastructure such as energy, transportation, and national defense. Third, visualizing model performance through line and bar graphs helps cybersecurity teams understand the advantages of RNN models over other algorithms, thereby facilitating decision-making regarding model selection for operational implementation. This shows that RNN development not only contributes theoretically but also has significant practical value for risk management and improving cybersecurity resilience in critical environments.

Although the RNN results are very promising, there are several limitations that need to be considered. First, RNN training requires relatively high computing capacity, especially on large and complex datasets such as CICIDS2020, so real-time implementation requires additional optimization. Second, this model still relies on the quality and representation of existing data; performance may decline if new attack data has patterns that are very different from the training dataset. The contribution of this research lies in demonstrating the effectiveness of RNNs for detecting various types of modern cyber attacks, with comprehensive evaluation using accuracy, precision, recall, F1-score, and AUC metrics, as well as comparisons with other algorithms. Future research could explore the integration of RNNs with attention mechanisms or hybrid models (RNN-LSTM-CNN) to improve the prediction of very rare or complex attacks. In addition, the implementation of RNNs in real-time critical defense systems could be tested to assess the direct impact on cyber attack response and mitigation.

4. CONCLUSION

This study successfully developed and applied a Recurrent Neural Network (RNN) model to predict cyber attacks on critical defense systems using the CICIDS2020 dataset. The evaluation results show that RNN outperforms other algorithms such as LSTM, Random Forest, and SVM on all key metrics, including accuracy, precision, recall, F1-score, and AUC. This superiority is related to the RNN's ability to capture long-term temporal patterns found in cyber attack activities, including rare attacks, so that the model is not only effective in detecting historical attacks but also adaptive to new attacks. A comparative analysis with previous studies confirms that RNNs are capable of delivering robust and consistent performance, even on more complex and diverse datasets such as CICIDS2020, thereby making a significant contribution to the literature on deep learning-based intrusion detection. Overall,

this study confirms that RNNs are an effective and adaptive solution for strengthening critical defense systems against evolving cyber threats. Based on the research findings, several suggestions can be made for further development. First, the implementation of RNN in real-time critical defense systems needs to be tested to assess the direct impact on cyber attack response and mitigation, including optimization of computing capacity and inference efficiency. Second, exploring the integration of RNN with attention mechanism techniques or hybrid models (RNN-LSTM-CNN) can improve detection capabilities against very rare or complex attacks. Third, further research can utilize more diverse datasets or live traffic data to test model generalization in real operational environments. Finally, the use of model performance visualization and interpretability, for example through feature importance or saliency maps, can support decision-making by cybersecurity teams and increase confidence in prediction systems. These suggestions are expected to expand the contribution of research in the development of proactive, adaptive, and reliable cybersecurity systems.

REFERENCES

Adeyeri, A., & Abroshan, H. (2024). Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era. *Information (Switzerland)*, *15*(11), 682. https://doi.org/10.3390/info15110682

Alijoyo, F. A., Kaur, C., Anjum, A., Vuyyuru, V. A., & Bala, B. K. (2024). Enhancing Cyber-Physical Systems Resilience: Adaptive Self-Healing Security Using Long Short-Term Memory Networks. *Proceedings - 3rd International Conference on Advances in Computing, Communication and Applied Informatics, ACCAI 2024*, 1–8. https://doi.org/10.1109/ACCAI61061.2024.10602467

Anwar, S., Zain, J. M., Zolkipli, M. F., Inayat, Z., Khan, S., Anthony, B., & Chang, V. (2017). From intrusion detection to an intrusion response system: Fundamentals, requirements, and future directions. *Algorithms*, *10*(2), 39. https://doi.org/10.3390/a10020039

Bilan, Y., Oliinyk, O., Mishchuk, H., & Skare, M. (2023). Impact of information and communications technology on the development and use of knowledge. *Technological Forecasting and Social Change*, *191*, 122519. https://doi.org/10.1016/j.techfore.2023.122519

Burmaoglu, S., Saritas, O., & Yalcin, H. (2019). Defense 4.0: Internet of Things in Military. In *Emerging Technologies for Economic Development* (pp. 303–320). Springer. https://doi.org/10.1007/978-3-030-04370-4_14

Dari, S. S., Thool, K. U., Deshpande, Y. D., Aush, M. G., Patil, V. D., & Bendale, S. P. (2023). Neural Networks and Cyber Resilience: Deep Insights into AI Architectures for Robust Security Framework. *Journal of Electrical Systems*, *19*(3), 78–95. https://doi.org/10.52783/jes.653

Díaz-Verdejo, J., Muñoz-Calle, J., Alonso, A. E., Alonso, R. E., & Madinabeitia, G. (2022). On the Detection Capabilities of Signature-Based Intrusion Detection Systems in the Context of Web Attacks. *Applied Sciences (Switzerland)*, *12*(2), 852. https://doi.org/10.3390/app12020852

Dr. Zeeshan Faisal Khan. (2025). Cyber Warfare and International Security: A New Geopolitical Frontier. *The Critical Review of Social Sciences Studies*, *3*(2), 513–527. https://doi.org/10.59075/k9cbhz04

Ghanem, K., Aparicio-Navarro, F. J., Kyriakopoulos, K. G., Lambotharan, S., & Chambers, J. A. (2017). Support Vector Machine for Network Intrusion and Cyber-Attack Detection. *2017 Sensor Signal Processing for Defence Conference, SSPD 2017*, *2017-January*, 1–5. https://doi.org/10.1109/SSPD.2017.8233268

Guerra, G. A. L. R. (2024). Contested Logistics as an evolution of military logistics using technological tools. *J. Comput. Electron. Sci.: Theory Appl.*, *5*, 5–27. https://doi.org/10.17981/cesta.05.02.2024.01

Gupta, R., Srivastava, D., Sahu, M., Tiwari, S., Ambasta, R. K., & Kumar, P. (2021). Artificial intelligence to deep learning: machine intelligence approach for drug discovery. *Molecular Diversity*, *25*(3), 1315–1360. https://doi.org/10.1007/s11030-021-10217-3

Islam, M. T. (2025). Adversarial Defence Mechanisms in Neural Networks for Ics Fault Tolerance: a Comparative Analysis. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *01*(01), 404–

431. https://doi.org/10.63125/xrp7be57

Khekare, G., Kumar, K. P., Prasanthi, K. N., Godla, S. R., Rachapudi, V., Ansari, M. S. Al, & El-Ebiary, Y. A. B. (2023). Optimizing Network Security and Performance Through the Integration of Hybrid GAN-RNN Models in SDN-based Access Control and Traffic Engineering. *International Journal of Advanced Computer Science and Applications*, *14*(12), 596–606. https://doi.org/10.14569/IJACSA.2023.0141262

Lehto, M. (2022). Cyber-Attacks Against Critical Infrastructure. In *Computational Methods in Applied Sciences* (Vol. 56, pp. 3–42). Springer. https://doi.org/10.1007/978-3-030-91293-2_1

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Mustafovski, R. (2025). The Use of Communication Platforms in Military Operations: Enhancing Strategic and Tactical Effectiveness. *Database Systems Journal*, *16*.

Padmavathy, R. (n.d.). *RNN-Based AI, Cloud Security, and Network Security in Banking: Strengthening Defence and Data Protection*.

Pătrașcu, P. (2021). Emerging Technologies and National Security: The Impact of IoT in Critical Infrastructures Protection and Defence Sector. *Land Forces Academy Review*, *26*(4), 423–429. https://doi.org/10.2478/raft-2021-0055

Rani, P., Kotwal, S., Manhas, J., Sharma, V., & Sharma, S. (2022). Machine Learning and Deep Learning Based Computational Approaches in Automatic Microorganisms Image Recognition: Methodologies, Challenges, and Developments. *Archives of Computational Methods in Engineering*, *29*(3), 1801–1837. https://doi.org/10.1007/s11831-021-09639-x

Raparthi, M., Soni, M., Tiwari, V., Dhumane, A., & Sharma, R. (2024). Scalable Implementation of Random Forests for Big Data Classification on Cloud Infrastructure. *International Conference on Deep Learning and Visual Artificial Intelligence*, 493–512. https://doi.org/10.1007/978-981-97-4533-3_38

Rosenberg, I., Shabtai, A., Elovici, Y., & Rokach, L. (2019). Defense methods against adversarial examples for recurrent neural networks. *ArXiv Preprint ArXiv:1901.09963*.

Sahin, C. B. (2021). DCW-RNN: Improving class level metrics for software vulnerability detection using artificial immune system with clock-work recurrent neural network. *2021 International Conference on INnovations in Intelligent SysTems and Applications, INISTA 2021 - Proceedings*, 1–8. https://doi.org/10.1109/INISTA52262.2021.9548609

Shafi, K., Abbass, H. A., & Zhu, W. (2006). An Adaptive Rule-based Intrusion Detection Architecture. *In the Security Technology Conference, The 5th Homeland Security Summit, Australia*, 345–355.

Sharma, B. P. (2024). Machine Learning-Driven Approaches for Contemporary Cybersecurity: From Intrusion Detection and Malware Classification to Intelligent Incident Response. *Nuvern Machine Learning Reviews*, *1*(1), 22–32. https://nuvern.com/index.php/nmlr/article/view/3

Sinha, P., Sahu, D., Prakash, S., Yang, T., Rathore, R. S., & Pandey, V. K. (2025). A high performance hybrid LSTM CNN secure architecture for IoT environments using deep learning. *Scientific Reports*, *15*(1), 9684. https://doi.org/10.1038/s41598-025-94500-5

Soe, Y. N., Feng, Y., Santosa, P. I., Hartanto, R., & Sakurai, K. (2019). Rule Generation for Signature Based Detection Systems of Cyber Attacks in IoT Environments. *Bulletin of Networking, Computing, Systems, and Software*, *8*(2), 93–97. http://www.bncss.org/index.php/bncss/article/view/113

Steingartner, W., Galinec, D., & Kozina, A. (2021). Threat defense: Cyber deception approach and education for resilience in hybrid threats model. *Symmetry*, *13*(4), 597. https://doi.org/10.3390/sym13040597

Usman, M. (2024). *Securing the Future: The Role of Neural Networks and AI in Advanced Cyber Defense Mechanisms*.

Vaseashta, A. (2022). Nexus of Advanced Technology Platforms for Strengthening Cyber-Defense Capabilities. *Practical Applications of Advanced Technologies for Enhancing Security and Defense*

Capabilities: Perspectives and Challenges for the Western Balkans, 14–31. https://doi.org/10.3233/nhsdp220003

Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep Learning Approach for Intelligent Intrusion Detection System. *IEEE Access*, *7*, 41525–41550. https://doi.org/10.1109/ACCESS.2019.2895334

Wei, Y., Jang-Jaccard, J., Sabrina, F., Xu, W., Camtepe, S., & Dunmore, A. (2023). Reconstruction-based LSTM-Autoencoder for Anomaly-based DDoS Attack Detection over Multivariate Time-Series Data. *ArXiv Preprint ArXiv:2305.09475*. http://arxiv.org/abs/2305.09475