ISSN: 0976-3376

Available Online at http://www.journalajst.com

ASIAN JOURNAL OF
SCIENCE AND TECHNOLOGY

*Asian Journal of Science and Technology*
*Vol. 17, Issue, 02, pp. 14161-14166, February, 2026*

RESEARCH ARTICLE

# COMPARATIVE ANALYSIS OF NEURAL NETWORK MODELS TO DETECT AND BLOCK OPEN WORLDWIDE APPLICATION SECURITY PROJECT VULNERABILITIES ON A WEB APPLICATION (AUTOMATED BLOCKING)

***Seyed Aliakbar Banialhossini and Dr. Reagan Ricafort**

School of Graduate Study AMA university

## ARTICLE INFO

***Article History:***
Received 19th November, 2025
Received in revised form
27th December, 2025
Accepted 08th January, 2026
Published online 24th February, 2026

***Key words:***

Open Worldwide Application Security
Artificial Neural Networks
Cyberattacks and Normal.

***Corresponding author:**
***Seyed Aliakbar Banialhossini***

## ABSTRACT

The goal of the current study is to conduct a comparative analysis of neural network architectures based on vulnerabilities identified by Open Worldwide Application Security Project in a web application context. This study comes from a descriptive and quasi-experimental model and is real data based empirical research. Moreover, in this study we identify the study as applied as the research aims to establish practical knowledge in a subject area. Our dataset is historical (post event), and the research design used is descriptive-correlational. We develop and analyze four different types of neural networks: Artificial Neural Networks (ANNs), Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs) and Hybrid Neural Networks (Hybrid NNs) in our experiment. To accurately predict, identify and block cyberattacks, the structures were trained on past internet usage data. The research design involved the design of the web page, data collection for cyberattacks and normal operational data, data cleaning, design of the neural network, training of the network, integration of the network inside the web page, blocking mechanism for malicious requests, and performance evaluation of the neural networks. The models resulted in precision, recall and F1 values, together with an area under the ROC curve of 0.98, that reflects their effectiveness in appropriately segmenting related data. Furthermore, none of the models showed a risk of overfitting since they had approximately identical accuracy levels for both training and validation set, with no significant discrepancies noted. After training using FLASK API the models were also added in web page. After running high-intensity OWASP ZAP attacks it was observed that this program can spot the attacks efficiently and block an end user by entering bad information. In addition, the predictive, detecting, and blocking of cyber-attacks by three neural networks at the same rate (NN, RNN, and Hybrid) was 90% and the entire attack frequency was observed. Index Terms: Web application security, artificial neural networks, convolutional neural networks, recurrent neural networks, hybrid neural networks.

**Citation:** ***Seyed Aliakbar Banialhossini.* 2026.** “Comparative analysis of neural network models to detect and block open worldwide application security project vulnerabilities on a web application (Automated Blocking)”, *Asian Journal of Science and Technology*, 17, (02), 14161-14166.

# INTRODUCTION

Cyber threats have grown significantly in number and complexity in recent years [1]. Cyber-attacks have increased exponentially and put millions at risk [2]: Various cyber security reports. Data breaches, ransomware, and advanced persistent threats (APTs) have targeted industries including finance, healthcare and critical infrastructure [3]. As the number of devices connected to the Internet expanded, the complexity of information technology ecosystems grew, and the capabilities of cyber criminals increased, cyber-attack incidents increased, all these factors contributed to a rise in the total number of cyber-attacks [4]. This is why protecting itself, end users and organizations against these types of cyber attacks are very important. Cybersecurity breaches can cause enormous financial loss, including the loss of revenue and reputation of economic institutions in financial institutions. In the field of healthcare, cyber-attacks may expose patients’ data, impair routine medical services, disrupt vital services like health care and can damage critical aspects of patient protection. Healthcare systems must pay dearly to the victims. The government agencies and critical resources providers are also targets for these attackers. Cyber-attacks against such organizations can have implications for public safety as well as national security [7]. Moreover, individuals are also at a high risk when personally identifiable information is compromised, resulting in identity theft and financial scams [8]. Increasingly common and sophisticated cyber-attacks against web applications results in severe data breaches and financial losses in many sectors. However, traditional cyber security becomes not sufficient, and advanced/intelligent security solution is required. To protect sensitive information and the continual and secure operation of digital services in all sectors from threats, advanced cybersecurity measures must also be implemented in order to ensure safeguarding. This study was undertaken as the urgent step to help the need to establish better ways to identify and block the Open Worldwide Application Security Project (OWASP) vulnerabilities that attackers use. Web applications have evolved into a digital underpinning technology [9], which is a modern form of digital infrastructure as such, which provides the vital services required for financial, healthcare and e-commerce functions that have also become an essential source of financial services and services offered today. But because of their accessibility and the data they use, they are also a breeding ground for cybercriminals. OWASP has classified the top ten weaknesses present today in web applications based on injection, broken authentication, and sensitive data leakages [10]. These vulnerable points are commonly exploited by malicious actors and are highly compromising of the security and integrity of web services. Conventional approaches, such as firewalls, intrusion detection systems (IDS), fingerprint based antivirus programs, have weaknesses in the detection and attack prevention of new and advanced threats [11]. These conventional approaches mainly use pre-set rules-based algorithms and are inadequate to defend against APT. As cyber-threats continue to develop, an adaptive and intelligent solution is needed to effectively identify a threat and protect its integrity. This study investigates the application in the application sphere of neural network classifiers—including convolutional neural network (CNN), recurrent neural network (RNN), and hybrid neural networks (HNN)—to solve these problems. Due to their features in learning from the information, finding patterns, predicting events etc in many scenarios, the techniques in neural networks also prove to be promising. In the cybersecurity domain, the models can be used for the recognition of attacks and detection of unusual events across web traffic, and consequently, enhancing the scope of the detection and prevention of cyber-attacks. A number of scientific theories discuss the use of neural networks in cyber security.

The theory of anomaly detection posits that malicious behaviour often deviates from what is observed from known norms. Patterns are statistically significant and thus detectable through statistical analysis and machine learning. Neural networks, particularly CNNs, can address pattern recognition issues and are used to discover anomalies in networking traffic [13]. On the other hand, the sequential data theory is of course key for the importance of analyzing time series for recognizing temporal patterns in cyber-based cyber attacks. Sequential data processing using RNNs also proves to be efficient in this task [14]. The hybrid model theory merges the benefits of the best features of the various neural network architectures for increased computation performance and accuracy [15]. This proposed research presents a study to determine the best neural network model for OWASP in web application to recognize and avoid the OWASP vulnerabilities based on comparison among CNN, RNN and HNN. In this research, these models are simulated and trained on real cyber-attack data. Performance evaluation of each model is made in regard to detection rate, blocking rate, occurrence of false positives and false negatives. We have carried out these experiments to contribute to strengthening cyber protection through empirical support on various types of learning neural models. This work has both scientific and practical implications on the applications of neural network applications in cyber security and offers several practical measures of enhancing the cyber security protection of web applications against cyber threats. These are significant learning points which organizations need to consider regarding the implications of their investments in a secure asset-preserving web systems in a cyber world. Further, the findings could also be directly applicable to other organizations, individuals and groups to be employed to prevent the impact of damage to other organizations, individuals and businesses from being compromised by cyber-attacks.

**Purpose and Description:** The growing number of global cyber-attacks has presented a global threat, exposing sensitive data along with financial losses to any web applications. The Open Worldwide Application Security Project (OWASP) offers serious weaknesses which hackers use to penetrate web systems. But traditional security measures are inadequate against complex increasingly difficult-to-defend threats. As a result, there is an urgent need for advanced and up-to-date security solutions to detect and block these threats in the best possible way. This paper targets using neural network models in web applications of different sizes—specifically convolutional neural networks (CNN); recurrent neural networks (RNN); or hybrid neural networks (HNN). Designed and analyzed in this way, this research seeks to highlight the best method for preventing and mitigating cyber-attacks.

**Operational Goals**

1. To design three neural network algorithms (CNNs, RNNs, and Hybrid NNs) on a web application for cyber-attack prediction
2. To identify cyber-attacks in a web application using three different neural network algorithms (CNNs, RNNs, Hybrid NNs).
3. To develop three neural network algorithms (CNNs, RNNs, and Hybrid NNs) to prevent cyber-attacks in a web application.
4. To inspect the detection rate of cyber-attacks inside a web application between CNNs, RNNs, and Hybrid NNs algorithms.
5. To evaluate the performance of CNNs, RNNs, and Hybrid NNs algorithms compared to a web application for blocking against cyber-attacks found.

***Significance of the Study:*** Cybersecurity is a global issue that has an impact on businesses, governments, and individuals. This research seeks to respond to a critical need in this realm, providing a solution for building better security mechanisms while maintaining and protecting digital infrastructure, data, and secure protocols. Cyber-attacks are growing in sophistication every single day and the need for dynamic and intelligent security systems. So-called neural networks with learning and adaptive capabilities are promising for threat detection and prevention solutions. This work would contribute to the design of such advanced security and provide web applications more robustness in dealing with cyber threats. Additionally, various neural network models have different strengths and weaknesses on data processing and analysis. Specifically, this paper studies CNNs, RNNs, and Hybrid NNs in relation to the highest rates of detection and blocking of cyber-attacks. The objective is to compare these three and, as a result, choose the best algorithm for the applications related to cyber security. The findings of this research have direct implications for web security. Organizations can use the most effective neural network model mentioned in this study to protect their web applications, thereby decreasing chances of incidents in network traffic or financial losses. Therefore, the research presents a model for how to use those neural networks in existing security solutions. From the viewpoint of the literature, this work broadens the knowledge about the application of neural networks in cyber security. This is a novel contribution to the threat detection literature involving machine learning, which can inform future research on novel security solutions. Comparative studies between different types of neural network models also contribute to the approach in the field. Furthermore, it demonstrates the importance of this research in bridging the gap between theoretical advancements and deployment of cyber security measures. Therefore, this work applies real world data and simulates real cyber-attack scenarios in order to validate that the neural network models proposed are theoretically sound and practically valid. This feature is crucial for industries that need powerful and scalable security solutions and adopt these models. Furthermore, this research promotes the cooperation between academia and industry, and the ongoing sharing of knowledge and creation of innovative cyber security technologies. This study improves the state of the art security of the web application, and lays an excellent foundation for future research efforts to fortify the digital infrastructure against the changing challenges of cyber.

**Scope and Limitation:** This research aims to investigate how neural network models are leveraged to discover, predict and prevent web application OWASP vulnerabilities through a neural network detection, prediction and blocking of OWASP vulnerabilities through CNN and RNN/HNN. The objective of this research project is to develop and study these models and investigate them to identify on whether to adopt the best methods for strengthening cybersecurity for modern cyber security against ever-changing cyber threats. This research investigates different models and compare them in the light of modern cyber threats to know the most promising methodology in designing and comparing them.

***Scope of Research***

**Neural Network Models:** This study is focused on only three types of neural networks – CNN, RNN, and HNN. They were selected for their successful uses in pattern recognition, sequential processing, and hybrid learning methods. This paper aims to build a framework to build these models for the purpose of extracting, predicting and blocking web application vulnerabilities found against the OWASP-identified web applications according to this model.

***OWASP vulnerabilities:*** The study specifically targets the top ten vulnerabilities against OWASP (OWASP vulnerabilities): injection, broken authentication, sensitive data exposure, etc., that target vulnerabilities which could have been exposed in web application vulnerabilities based on OWASP-named OWASP vulnerabilities. These vulnerabilities are usually exploited by attackers to get access to web applications.

***Detection and blocking cyber-attacks:*** One very important research focus area today is in the detection and blocking of cyber-attacks through neural networks. This paper evaluates the models' performance on the detection frequency, blocking and false positives and negatives, according to which the most important metrics measure their ability to classify models.

***Dataset:*** The research works on real-world and simulated data to train and test models for constructing neural network models. The reason that it is being pursued by this way is that this model has the effect of ensuring that research findings are relevant to the real world, i.e. it is practical and can be used in practice.

***Comparison:*** This paper compares CNNs and RNNs & HNNs to detect cyber-attacks through detection and blocking. Its aim is to find a model with the best performance criteria and make recommendations regarding its application in web application security.

***Limitations***

1. Generalization of the models The generalisation of neural network model is also hampered by the range of datasets used and its quality and quantity. When the dataset is not comprehensive in terms of attack models if attack pattern and scenarios are not common and many not in model that can fit easily to detect the unseen threat.
2. Computational resources: Training and evaluating neural networks, especially deep learning models, such CNN and RNN, demands substantial computing resources. Access to resources like these could hinder the scope of this research, and thus model complexities or depth, that can be built.
3. Research on OWASP Top Ten: OWASP vulnerabilities are important, but this research focuses on the top ten categories of OWASP. Not addressing all of the security vulnerabilities other than OWASP may not be relevant generalizable to the wider research.
4. Existing timeframes: The time frame of this study may not allow for the iterative refinement and testing of models. This restricts the reliability and accuracy of the models in practical scenarios.
5. Emerging threat landscape: Cyber-attack environments are not static. The models built in this study may be less productive as attackers create new strategies to bypass existing security protocols on an ongoing basis.

# RESEARCH METHODOLOGY

This study is quasi-experimental. In the realm of empirical studies, it is also based on genuine information. Additionally, considering its purpose it is included in applied research, as that is the purpose of applied research is to develop applied knowledge in a special area. The type of research data is real-time data. We present the research approach and gather the research methodology to test the research questions and the data for these tests, conducting proper statistical operations on neural networks to investigate and analyze. We are finally able to find an accurate solution for the questions in this research by going through these data to solve its correct answer. Data analysis is a multiple step process where in which data collected in various ways is made up, categorized and then converted into data to establish relationship between data and provide scientific analysis. It is a process of conceptual and empirical refining of the data, in which multiple statistical techniques and neural network systems are used for generalizing. Depending on the type of data, the kind of theorizing and tools of data collection, analysis processes differ by category and research types. Four neural networks are applied, namely: artificial neural networks (ANNs), convolutional neural networks (CNNs), recurrent neural networks (RNNs) and hybrid neural networks (hybrid NNs) which we experiment with and this is based on the website activity data from past. These neural networks are built and trained to predict and detect cyber-attack and prevent them. Networked to study in this paper selected the neural network as identified in literature review. For example, Tekerek, A. (2021), Al-Milli, N., & Hammo, B. H. (2020, April), and Jemal et al (2021) used CNNs algorithm; Yenduri, G., & Gadekallu, T. R. (2022) and Tang, L., & Mahmoud, Q. H. (2021) used RNNs algorithm.

**Research Process**

The steps of the work are taken like this:

- Website design
- Normal data about site is collected
- Establishment of blocking systems for suspicious requests
- Gather cyber attack-related data
- Cleaning and prepping data (ordinary data and suspicious data)
- Neural Network algorithms (Artificial Neural Networks (ANNs), Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs) and Hybrid Neural Networks (Hybrid NNs))
- Integrating the trained algorithms to the Web site
- Set up blocking mechanisms for suspicious requests
- Benchmark neural networks for effectiveness

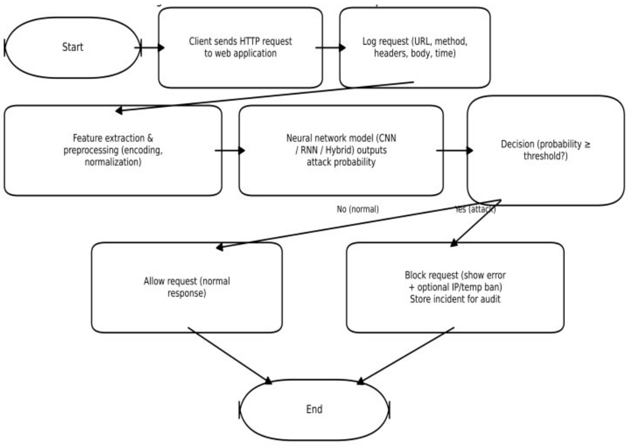
Start
Client sends HTTP request to web application
Log request (URL, method, headers, body, time)
Feature extraction & preprocessing (encoding, normalization)
Neural network model (CNN / RNN / Hybrid) outputs attack probability
Decision (probability ≥ threshold?)
No (normal)
Yes (attack)
Allow request (normal response)
Block request (show error + optional IP/temp ban) Store incident for audit
End

**Fig. 1. Flowchart of AI-Based web intrusion detection and prevention**

**Get data from the site**

Data cleaning and preparation
Natively trains a neural network with collected data
Real-time data processing
Detection result
No → Normal data → Continue normal work stream of the website
Yes → Attack detection → Website error message display → Admin alert

***Data Collection Methods:*** Theoretical resources, literature, and theoretical topic of the research has been gathered by library resources. Due to its design, normal data and information collected regarding Cyber-Attacks from a site that was created for the purpose of this part of the research is used for research purposes. Sites data contains data produced from user interaction on the site. Site data is being utilized for analyzing users' behaviours, optimizing server performance and detecting cyber-attacks. These consist of logs and data related to HTTP requests and responses made in user interactions, or on other systems with the web server. The data of this study consists of two types. Normal data and attack data. This data includes Requests, Responses, Metadata data, which are expressed as:

Requests data consists of HTTP method, desired URL and set parameters as well as time in which it will send it. Response's data, comprising the HTTP status code, content and volume of the reply as well as other relevant information. Metadata includes information about sources (such as IP), browser type, as well as metadata pertaining to the request. Usually we obtain this from the web server, security analytic tools and site users. Site server data provides details of each HTTP request, the style, URLs, response time. Tools such as OWASP ZAP are also used to investigate suspicious requests or attacks. In this study, this tool was utilized to gather ten kinds of attacks on the website along with a few examples. In addition, an interaction between a browser or client and the server is logged. Lastly, some of the data is classified by two classes: Normal Data and Attack Data. Normal Data is legitimate and non-fearing requests received from normal users interacting via the site or legal services in return, and Attack Data includes those that might have been sent intending to harm or abuse. From collected data, the following features are extracted and used by machine learning algorithms:

**Table I. Features Definition**

| Features | Definition |
|---|---|
| Method | HTTP request method. Like GET, POST. |
| URL_Length | URL length is the number of characters in the URL. |
| URL_Param_Count | The number of parameters in a URL that usually appear in the URL's query string. |
| HTTP Response Code | HTTP response code. Like 200 for successful, 404 for not found, etc. |
| Reason | Explanatory text for the HTTP code (such as OK, Not Found). |
| RTT | Request response time (ms). |
| Size Resp. Body | The size of the response body is the size of the response content in bytes. |
| Highest Alert | Warning level. Like Low and Medium. |
| Tag | Text labels are for answers. Like Script, Comment, JSON. |
| Size Resp. Header | The size of the response header is in bytes. |
| Timestamp | The date and time of sending the request. |

**Table II. Data Quantification Method**

| Features | Data quantification method |
|---|---|
| Method | It becomes quantitative with OneHot Encoding or Label Encoding. |
| URL_Length | It is a quantitative feature and its length indicates the possibility of suspicious attacks. |
| URL_Param_Count | It is a quantitative feature. |
| HTTP Response Code | It is a quantitative feature. |
| Reason | With OneHot Encoding, it is converted to a numeric attribute and used as a category. |
| RTT | The feature is numerical and needs to be normalized. |
| Size Resp. Body | The numerical feature is suitable for analysis. |
| Highest Alert | With OneHot Encoding, it is converted to a numeric attribute and used as a category. |
| Tag | With OneHot Encoding, it is converted into a numeric feature and each tag is modeled as binary (1/0). |
| Size Resp. Header | It is a quantitative feature. |
| Timestamp | Converts to attributes such as time of day, day of week, or time pattern. |

**Data Analysis:** In order to analyze the information, the following algorithms were used:

1. Artificial Neural Networks (ANNs)
2. Convolutional Neural Networks (CNNs)
3. Recurrent Neural Networks (RNNs)
4. Hybrid Neural Networks (Hybrid NNs)

These algorithms were implemented in the Python programming language along with Google Colab programming environments

***Performance of Neural Networks:*** Assembled based on the code, a neural network was executed, using CNNs and the resulting parameters like the speed, reliability, and accuracy. In this section we consider training results obtained from 4 neural networks; namely, artificial neural networks (NNs), convolutional neural networks (CNNs), recurrent neural networks (RNNs), and hybrid neural networks (Hybrid NNs). These networks are trained on data from the site including normal and attack data. This means that normally collected data, but also attack data, will be used to make the networks trained. The models are then further studied and analyzed for their performance in detail, including accuracy and error statistics, and graphs (training process), confusion matrix, ROC and Precision-Recall curve. The analyses should analyze how well the model is learning during the process of training and validation, looking for possible overfitting, checking the balance of data, understanding the performance of the model in terms of true and false positive/negative rate, and describe what worked well by the current model as well as what didn't.

***Neural Networks (NNs):*** After training the neural network model, the pattern of the training accuracy with increasing sequence time and decreasing bias of the model can be concluded. The validation set accuracy also increased through our training along with the training and, after a few epochs, settled pretty close to a value, which proves that the model learned the patterns out of the dataset. The accuracy values from training and validation at the point of termination were nearby which indicated that the model was trained well and it was able to identify attack data in contrast to normal data. Fig. 2. We trained and validated the neural network model over epochs. The Learning Curve shows the performance of training the neural network for the duration of 50 epochs. The model accuracy is left, the training and validation accuracy rises sharply to 90% (in the initial epochs), the high performance and fast learning of the model. The right is the value loss of the model on the training set and the validation set.

It is evidenced that the model loss decreases very fast early in the training period and then settles down within ranges closer to zero, making the model minimize error. At the same time, the validation loss can also be very closely maintained at a low value to ensure the model is generalizing very well without overfitting. That tells us that the model is actually doing exceptionally good with quite negligible difference and even zero losses or even negative losses.

***Convolutional Neural Model (CNN):*** The Convolutional Neural Network (CNN) model ran great success based on more than 50 training units. In the beginning, the model had only 0.8041 accuracy when training was running, after a few sessions it shot up to 90% and all the subsequent sessions the model kept its accuracy fixed of 90%. Finally, in the early sessions, model loss was well minimized (highly limited), and near zero, and thus the learning of the model was effective as well as optimal. The precision, recall, and F1 were 0.95 respectively for the classification for both class 0 and class 1, indicating the very good precision and performance in the test set of the proposed model. These results demonstrate the model works perfectly and completely efficiently in classifying cases of both classes. Fig. 3. Training and validation performance of the convolutional neural network model across a set of epochs.

***Recurrent Neural Network (RNN):*** Training was similarly performed in this model and the learning curves are indicated as follows: Fig. 4. Training and validation performance of the recurrent neural network model over epochs. The accuracy plot is left during the training time and validation time. The training accuracy (blue line) and validation accuracy (orange line) were 90% after the first period and stable for the consecutive periods. That means that the model learned very fast and got away with identifying the data well. The model loss changes for each of the periods are shown in the right graph. The model loss (blue line) decreases significantly from the start of the training then reaches the smallest value, almost zero. This suggests that the model is relatively fast as the best learning state and it is making the least error. The validation loss (orange line), too, performed similarly to say that it was not overfitting (validating). These outcomes reflect perfect model performance, accuracy is 90%, which is in the range of 95% and loss virtually zero for training and validation data.

***Hybrid Neural Network (Hybrid NN):*** With the architecture of CNN and RNN Hybrid NN model it was able to achieve 95% accuracy after 50+ training. The predictive power of the model started at 74.29%, while it was 95% after the first session, and it remained so for the next ones. Moreover, its loss value decreased from 0.5025 in the initial sessions to near zero in the final sessions, demonstrating rapid accurate learning of the model. Even in validation set, even 95% accuracy was observed and then loss near zero indicating no overfitting which suggests that the model is able to generalize fairly well for the new data. Fig. 5. We plot the hybrid NN model between training and validation epochs in this work (up to 50 epochs). The performance for the CNN+RNN hybrid model on 50 training sessions is presented in the given graph as shown in these plots. From the left plot, we can find the accuracy of the model during training sessions and validation sessions. Blue line and orange line (training accuracy and validation accuracy) are the values 95% and remaining constant, respectively, at the end of the 1st session, showing that the model learned quickly and well. Model loss variation can be seen by the suitable graph. Model loss (blue curve), drastically decreases early in the training process and then drops towards near zero value with very low value, showing high-speed model optimization and accurate model adaptation. Also on validation, (orange line) loss is also declining at a rapid rate, indicating the absence of overfitting and good model performance to generalize to new data, respectively. All these results imply highly strong and perfect model fit on validation and training.

***Detection Performance and Blocking Performance Comparison:*** For all the models covered in this paper precision, recall and f1 significance were studied. There was none of the errors (in class prediction) in the confusion matrix therefore all the samples were identified correctly. The likelihood of overfitting of the models was also taken into consideration, and the overfitting rate was investigated at a very low level. Detection strength and the ability to prevent on-network attacks comparison of neural network models applied. FLASK API-trained models were used on the site. After carrying out OWASP ZAP attacks with high frequency, it was observed that this program had adequate detection of attacks and was capable of blocking the user through the threat information inputs. All of the 4 neural network models were used on the site and detected and stopped all of the attacks. The threshold of the entire set of operating algorithms was taken as 0.7, which would allow these algorithms to be compared. Fig. 6. Comparison of the performance of algorithms in detecting and blocking cyber attacks. According to the results, the best performance is compared to the RNN algorithm, with 98.70 percent detection power. After that, the best performance was associated with the NN algorithm with 93.54 percent detection power, then the Hybrid algorithm with 92.90 percent detection power. Next, all detected cyber-attacks were blocked. The accuracy of predictors (MSE/frequencies of the data) was very high. The total accuracy of NN, RNN, and Hybrid models for predicting, detecting and blocking cyber-attacks is 90%. As a whole, the various algorithms (neural network, convolutional neural network, recurrent neural network, hybrid model) had similar and excellent performances in recent experiments.

# DISCUSSION AND CONCLUSION

New artificial and deep neural networks have become very strong new tools in cybersecurity over the last few years. In tests using four different neural network architectures (ANN, CNN, RNN and Hybrid) on an intrusion detection system, we found that these models distinguished between normal data and malicious. The results indicated that all of our models achieved an accuracy and performance of 0.98 in the training and validation procedures. This is a reflection of the quality of the input, accurate feature selection and the learning process. But what separates the models from each other is their ability to perform real-life scenarios like running a command on OWASP ZAP attacks and responding to an API based on FLASK API. At the same time, we showed that the recurrent neural network (RNN), based on a sequential structure and internal memory, has the highest attack detection rate (98.70%) of all models. This outcome demonstrates the strong performance that RNN possess in analyzing structured data and numerical features. Both the training and evaluation stage fully converge, thus signifying the stability of the model, the ability to learn effectively, and the lack of overfitting. Through the combination of CNN and RNN architectures, the HNN model can simultaneously exploit CNN's feature extraction capacity and RNN's temporal memory. The model is characterized by very high performance, fast convergence and good indicators-balance. While its API analysis detection was just 92.90%, which is lesser than ANN and RNN, the deep understanding and multi-layer of the input data mean it's more suitable for more complicated data. CNN is widely used in image, spatial data and provides the correct results in the theoretical and training phase in this research. This model has 90% accuracy on all the indicators, and the speed at which we decreased the loss value shows that if we transform the data into an analyzable structure by using convolutional layers, this model can become one of the effective tools for detecting cyber threats.

But this model produced unacceptable results in practice and on-site environment. Model accuracy was perfect in laboratory, but performed differently in the real environment, thereby illustrating the necessity of understanding the fit of models with respect to real life environments and dynamic cyber attacks. RNN was very good at identifying patterns of sequences as well as understanding the temporal structure of attacks. Integrating with HNN architecture can be very useful for example applications like Log analysis with text and time information. Despite being simpler than any other models, the performance of ANN model was satisfactory. This conclusion indicates that its complexity is not necessary for appropriate performance. Conversely, matching data features to the model and training quality are two equally critical. Full AUC (0.98) for all models in the ROC curve indicate excellent resolution and performance in identifying two data classes (normal and malicious). Thus, the most significant takeaway from this analysis is that a model selection algorithm, when perfect in accuracy, precision, recall, F1 and AUC is required, is not sufficient for such selection. What matters in reality with real operation is stability, response time and immunity from unknown attacks.

### Suggestions for Future Research

- Based on the results, it is recommended that in designing hybrid models of cyber-threat prevention, the combination of ANN and RNN modeling in a two-stage (waterfall) design is adopted.
- It was also recommended that in RNN and hybrid models, the number of middle layers should be increased and performance should be measured and compared by concentrating on the few critical features.
- In the light of the promising results based on the neural networks being applied, other kinds of training algorithms should be adopted in the future to improve the model to withstand the sophisticated attacks.

# REFERENCES

Bennett, B. T. Understanding, Assessing, and Responding to Terrorism: Protecting Critical Infrastructure and Personnel. John Wiley & Sons, 2018.

Fernandes B. and K. Mannepalli, "Speech Emotion Recognition Using Deep Learning LSTM for Tamil Language," Pertanika Journal of Science & Technology, vol. 29, no. 3, 2021.

Gangwar S. and V. Narang, "A survey on emerging cybercrimes and their impact worldwide," in Research Anthology on Combating Cyber-Aggression and Online Negativity, IGI Global, 2022, pp. 1583–1595.

Joseph, P. T. E-commerce: An Indian perspective. PHI Learning Pvt. Ltd., 2023.

Koyame-Marsh R. O. and J. L. Marsh, "Data breaches and identity theft: Costs and responses," *IOSR Journal of Economics and Finance* (IOSR-JEF), vol. 5, pp. 36–45, 2014.

Lane, T. D. "Machine learning techniques for the computer security domain of anomaly detection," Ph.D. dissertation, Purdue University, 2000.

M. Aljabri, M. Aldossary, N. Al-Homeed, B. Alhetelah, M. Althubiany, O. Alotaibi, and S. Alsaqer, "Testing and exploiting tools to improve OWASP top ten security vulnerabilities detection," in 2022 14th International Conference on Computational Intelligence and Communication Networks (CICN), 2022, pp. 797–803.

Munk, T. The Rise of Politically Motivated Cyber-Attacks: Actors, Attacks and Cybersecurity. Routledge, 2022.

Perera, S. X. Jin, A. Maurushat, and D. G. J. Opoku, "Factors affecting reputational damage to organisations due to cyberattacks," Informatics, vol. 9, no. 1, p. 28, 2022.

Stewart, J. M. Network security, firewalls and VPNs. Jones & Bartlett Publishers, 2013. [12] D. A. Bird, Ed., Real-time and retrospective analyses of cyber security. IGI Global, 2020.

Toledano, S. A. Critical Infrastructure Security: Cybersecurity Lessons Learned from Real-World Breaches. Packt Publishing Ltd., 2024.

Triplett, W. J. "Cybersecurity Vulnerabilities in Healthcare: A Threat to Patient Security," Cybersecurity and Innovative Technology Journal, vol. 2, no. 1, pp. 15–25, 2024.

Verma R. and C. Shri, "Cyber security: A review of cybercrimes, security challenges and measures to control," Vision, 2022.

Yenduri G. and T. R. Gadekallu, "Recent Advancements in Network and Cyber Security Using RNN," in Trust, Security and Privacy for Big Data, pp. 129–143. CRC Press, 2022.

Zhang, Y. H. Lin, Z. Yang, J. Wang, S. Zhang, Y. Sun, and L. Yang, "A hybrid model based on neural networks for biomedical relation extraction," *Journal of biomedical informatics*, vol. 81, pp. 83–92, 2018.

*******