An Improved Machine Learning-Based Model for The Identification and Management of Zero-Day Attacks in A Cloud-Based Network

NNADI LINDA C.[1], ASOGWA T.C.[2]
[1,2] *Computer Science Department, Enugu State University of Science and Technology*

Abstract- ***Zero-day attacks pose significant challenges to modern cybersecurity systems due to their unpredictable nature and ability to bypass traditional detection mechanisms. Therefore, this study presents an improved machine learning-based model for the identification and management of zero-day attacks in a 5G cloud-based network. The proposed system integrated an Artificial Neural Network (ANN) model with a real-time threat isolation framework based on a novel data model made up of anomaly-based, behavioural and signature-based features. Data was collected from the Litcoder Cloud in Enugu, Nigeria and then the data was pre-processed through visualization, imputation and normalization techniques. An online adaptive feature selection mechanism using Online Recursive Feature Elimination (ORFE) was further employed to dynamically prioritize relevant threat features. The ANN model presented in this study was trained using a backpropagation algorithm with dropout regularization and evaluated using performance metrics including accuracy, precision, recall, F1-score and confusion matrix. Simulation on a 5G cloud-based environment demonstrated an average threat detection time of 0.8 seconds, high throughput of 85.10%, low CPU utilization of 0.403 and minimal latency of 27.07ms. The model achieved high classification accuracy of 98.5% and demonstrated resilience in real-time conditions, validating its capability for proactive threat detection and mitigation.***

Indexed Terms- ***Zero-Day Attacks; Machine Learning; ANN; Threat Isolation; 5G Cloud Network***

I. INTRODUCTION

The adoption of cloud computing represents a paradigm shift in the way organizations operate, enabling them to achieve greater agility, efficiency, and innovation in today's fast-paced digital economy. While cloud computing offers the aforementioned benefits, Oduah *et al*. (2023) argued that it also has several challenges, which include system vulnerability (Patzke, 2022), congestion (Nweke *et al*. 2023), and cyber-attacks (Talpur *et al*. 2024).One of the key benefits of cloud computing, according to Safdar *et al*. (2022), is its ability to provide elastic and scalable resources, allowing users to scale up or down based on their computing needs. This scalability enables businesses to handle fluctuating workloads efficiently, ensuring optimal performance and resource utilization while minimizing costs. Additionally, Dwivedi *et al*. (2019) posited that cloud computing eliminates the need for large upfront investments in hardware and infrastructure, as users pay only for the resources they consume on a pay-as-you-go basis. Another advantage of cloud computing is its inherent flexibility and accessibility (Kaur *et al*. 2018; Aljuaidand Alshamrani, 2024). With cloud services, users can access their data and applications from anywhere with an internet connection, using a variety of devices, including laptops, smartphones, and tablets (Namasudra*et al*. 2020). This accessibility facilitates remote work, collaboration, and innovation, empowering organizations to adapt to changing business requirements and market dynamics more effectively (Tu *et al*. 2018).

According to Dwivedi *et al*. (2022), one of the challenging experiences in cloud computing technology is the issue of cyber-attacks. Cyber threats are attacks tailored towards illegal and

unauthorized access to the cloud-based network, with the aim of ransomware and stealing information for financial gain. Among the diverse strategies for cyber-attacks, Vetterl and Clayton (2019) revealed that zero-day continued to gain increased attention in the research community.

Over the years, numerous studies have addressed the management of zero-day exploits and attacks, with a significant portion focusing on the application of deep packet inspection (Deri and Fusco, 2021) and deception technologies (Ilg *et al*. 2023). However, a critical gap persists in the necessity for a dependable cybersecurity framework for handling zero-day attacks. The deception approach customizes cybersecurity techniques to divert intruders' attention from the original network (Amv42, 2018), while deep packet inspection concentrates on monitoring incoming packets for features that may indicate confidentiality breaches (Deri and Fusco, 2021).

Machine Learning (ML) has emerged as a powerful tool in cybersecurity, offering advanced capabilities for threat detection, anomaly detection, malware analysis, and risk assessment (Sochima et al., 2025; Habor et al., 2021; Patil, 2019). ML algorithms can analyze vast amounts of data, identify patterns, and make predictions to enhance cyber threat intelligence and improve security posture (Nkongolo *et al*. 2022). However, the integration of ML into cybersecurity also brings forth several challenges and considerations that must be addressed to maximize its effectiveness and mitigate potential risks.By leveraging ML techniques, cybersecurity professionals can automate threat detection processes, detect previously unseen threats, and respond to security incidents in real-time. ML models can learn from historical data, adapt to evolving threats, and improve accuracy over time, making them valuable assets in defending against sophisticated cyberattacks (Li *et al*. 2022).

While numerous studies have made significant progress in the classification and response to zero-day attacks, existing approaches like Erskine (2025) and Ismail (2025) focused on isolated aspects of threat detection either anomaly-based, behavioral, or signature-based methods. However, there is a noticeable absence of comprehensive models that integrate all three categories of zero-day threat features (anomaly, behavioral, and signature-based zero-day threats) within a unified framework. This fragmented approach limits the robustness and adaptability of detection systems, especially in complex and dynamic environments like cloud computing. Therefore, there is a critical need to develop an integrated threat detection model that simultaneously considers these diverse feature classes to improve detection accuracy, reduce false positives, and enhance response efficiency against zero-day attacks in cloud. Therefore, this paper is focused on developing an improved machine learning model for the management of zero-day attacks in a cloud computing environment.

II. RESEARCH METHODOLOGY

The methodology used for this work is the extreme programming approach. In realization of the study aim, data was collected considering different classifications of zero-day attacks and then processed before the online feature extraction process. In realizing this purpose, a data model that captures the intricate behavior of zero-day attack features will be designed, and then dynamic feature engineering techniques that will focus on extracting features of evolving threat landscapes will be proposed. This will be applied to train an improved machine learning algorithm designed to address issues of overfitting and learning bias while generating a model for the detection of zero-day threats.

2.1 The Proposed Zero-Day Attack Identification and Response

The proposed zero-day attack identification and response system will be developed in this work considering machine learning algorithm and an improved zero-day data model. The major components for the study are data collection, data processing, proposed online feature extraction, machine learning algorithms, training of the algorithm, classification results as shown in the block diagram of Figure 1.

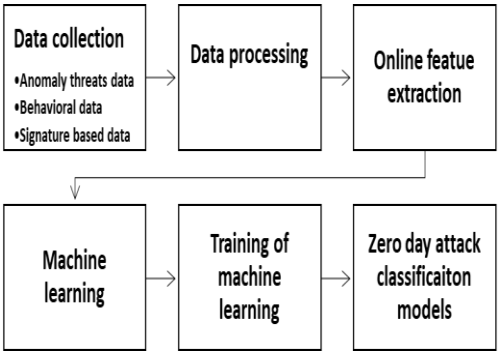

Figure 1: The proposed zero data attack classification results

The Figure 1 presents the proposed system developed with the new data model made of anomaly features, behavioural features, and signature-based features. The data were processed and then the feature vectors extracted online in real-time to feed three selected machine learning algorithms which are neural network, decision tree, and random forest respectively. The algorithms will be trained to generate the classification model for zero-day attack.

2.2 Data collection

The data used for this work was collected from Litcoder Cloud located at Asata, Enugu 400001, Enugu. The data considered is anomaly features which model the network behaviour under diverse threat conditions such as normal, anomaly, signature and behavioural from 2021 to 2024. The data sample for anomaly is 42,120 features span across 8 attributes. The signature- based samples contains 48,892 features span across 7 attributes, the behavioural-based data contained 40,502 features which is spanned across 8 attributes, while normal packet contain 40593 features. The total sample size is of attributes in the new data model is 172,107.Figure 2 presents the location of the data source.

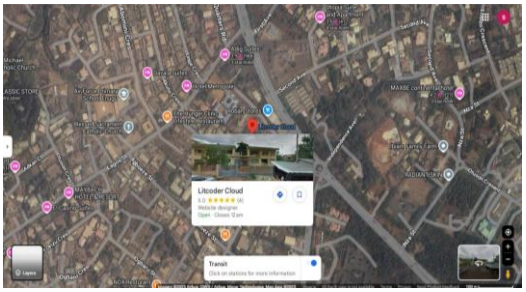

Figure 2: The data source in Google Map (Source: Google Nigeria)

2.2 Data processing

The new data model was processed through visualization, imputation and normalization. The data visualization was carried out in python programming environment using exploratory data analysis tool to model and understanding the relationships between attributes and how they impact on system behaviour. The imputation approach applied was mean imputation technique which computes the mean value of the mission data row column and then predicts the value. Finally, the normalization approach applied is the Min-Max normalization technique. This ensures that features dimension is reduced, addressing issues of overlapping features and maintaining data quality.

2.3 Online Adaptive Feature Selection and Extraction Model to Prioritize Threat Feature Detection from Incoming Packets

Online adaptive feature selection and extraction model is proposed or the prioritization of threat feature detection from incoming packets.The model defines the features spaces of the packet features as F= $\{f_1, f_2, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots f_n\}$; these features include the behavioral, anomaly and signature-based features from the new data model. Let the dynamic feature set e represented as S_t where t is the time series. The initial feature weights is set based on entropy ranking, then Online Recursive Feature Elimination (ORFE) technique is applied to identify the most relevant weights using Equation 1;

$$W_t(f_i) = W_{t-1}(f_i) + \propto . I(f_i, Y_t) \qquad (1)$$

Where $I(f_i, Y_t)$ is the mutual information of features f_i with the targetY_t and learning rate $\propto$. The irrelevant features are removed when $W_t(f_i) < \tau$;

where τ is the threshold for the feature elimination). To monitor incoming packets, and identify new dynamic features, f_j, this is determined when $W_t(f_i) > \tau$. The new feature is added to S_t.

Feature selection algorithm

1. Start
2. Initialize parameters
3. F= $\{f_1, f_2, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots f_n\}$ %% $dataset\ features$
4. Represent dynamic feature set as S_t
5. Measure feature relevance %% Apply ORFE
6. Apply $W_t(f_i) = W_{t-1}(f_i) + \propto .I(f_i, Y_t)$ for weight adjustment
7. Apply $W_t(f_i) < \tau$ %% To remove irrelevant features
8. $W_t(f_i) > \tau$ %% To identify new features
9. Add new features to S_t
10. Return to Step 4

End

2.4 Neural network Training for the classification of Zero-Day Attack using Python

Neural network is a machine learning algorithm which is developed with several neurons, activation function and layers. The type of neural network used is multiple layered neural network (Li and Yan, 2024). The activation function used is sigmoid, the training algorithm used is back propagation, and the regularization model used is dropout (Kekong et al., 2019; Sarikaya and Hinton, 2019). The number of input to the neural network is 13, the number of hidden layer neurons is 30 and the output layer is 2. The neural network was trained in python programming environment, using the dataset for zero-day attack detection (Sarikaya and Hinton, 2019).The ANN model was trained using back-propagation algorithm, where input features were processed through multiple hidden layers, and weights were updated and minimize classification loss.

2.5 The performance evaluation metrics

To assess the effectiveness of the trained models in detecting dynamic zero-day attacks, various performance evaluation metrics were employed. Accuracy was used to measure the overall correctness of the models in classifying attacks and normal traffic. Precision was calculated to determine the proportion of correctly identified zero-day attacks among all predicted attacks, ensuring a low false positive rate. Recall measured the ability of the model to correctly detect zero-day attacks, minimizing false negatives. F1-score, the harmonic mean of precision and recall, provided a balanced evaluation, especially when dealing with imbalanced datasets. The models' performance was further validated using confusion matrices, which provided insight into true positives, false positives, true negatives, and false negatives, ensuring a comprehensive assessment of detection accuracy.

2.6 Model for the classification of dynamic Zero-day attack

The model or the classification of the zero-day attack is the outcome of the training process. This model was generated after loading the machine learning algorithms with data and then train to generate the model for the detection of dynamic zero-day attack. The model upon generation was compared for all ML algorithms and the best identified and then applied for the monitoring and detection of zero-day attack.

2.7 Threat Isolation Model

The threat detection model is developed with the aim of isolating the classified threat from the cloud computing environment to prevent its impact during attack. The model was developed with the classification model as the input. Upon classification of packet as zero-day attack using the label of behavioural, signature and anomaly, the IP address of the user is detected and then block from access to the server, while if the data is classified as normal packet, it is allowed access to the server. The isolation algorithm is presented as follows while the flowchart was presented in figure 3;

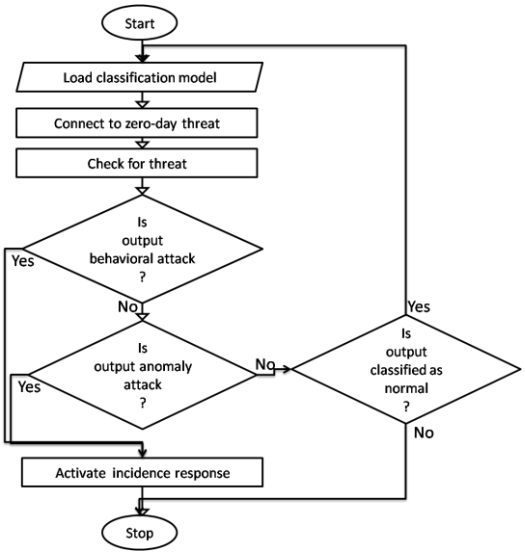

Figure 3: Flowchart of the isolation algorithm

2.8 The Improved Machine Learning Model for Dynamic Zero-Day Attack Management

This section presents the new security model, which was designed with a combination of the classification model and also the threat isolation model as in figure 4. From the results, it was observed that the integrated model significantly enhanced the detection accuracy and response time compared to traditional static approaches. The classification model was responsible for the rapid identification and categorization of previously unseen attack signatures, while the threat isolation model ensured that once detected, the malicious activities were contained in real-time to prevent lateral movement or system compromise.

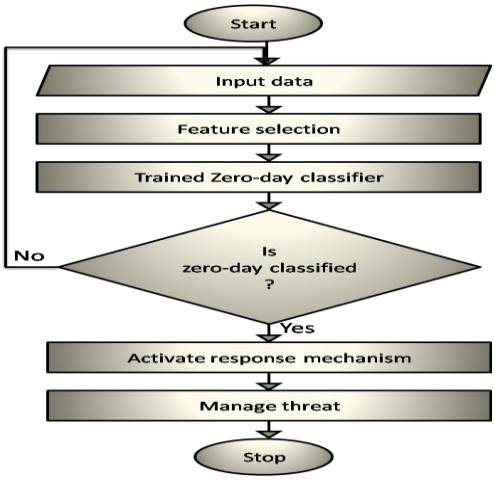

Figure 4: Flowchart of the new zero-day attack detection system

The dynamic nature of the system allowed it to adapt to evolving threat landscapes by leveraging continuous learning techniques and anomaly detection strategies. The model achieved a higher true positive rate, minimized false alarms, and maintained consistent performance under varying network loads. Moreover, the deployment of the threat isolation component enabled proactive mitigation, reducing the overall impact of zero-day exploits.

Experimental evaluation showed that the system outperformed baseline machine learning models in terms of precision, recall, and F1-score. Furthermore, it demonstrated robustness in both simulated and real-time environments, confirming its practical applicability in modern cybersecurity infrastructures. This validates the model as a reliable framework for real-time zero-day attack management in dynamic and distributed network environments.

2.9 Simulation of the model on 5G cloud-based Network

The simulation of the zero-day detection model on a 5G cloud-based network is conducted by integrating the trained ANN model into the network security framework. The model continuously monitors network traffic, analysing key parameters such as bandwidth utilization, packet loss, jitter, and latency to detect anomalous behaviours associated with zero-day attacks. When an anomaly is detected, the model classifies it as either a normal or attack packet, allowing for real-time threat mitigation. This simulation ensures that malicious traffic is promptly identified and isolated, preventing unauthorized access and system compromise while maintaining network performance. The implementation demonstrates that with the ANN model in place, throughput remains high, latency is minimized, and packet loss is significantly reduced compared to an unsecured network. To further evaluate the effectiveness of the zero-day detection model, performance xmetrics such as TPR, FPR, detection time, and CPU utilization are analysed. This simulation validates the feasibility of deploying intelligent machine learning models in real-time 5G security frameworks for proactive threat prevention.

III. RESULT OF ANN TRAINING

The result of the neural network training was reported in the section to evaluate the performance. The training process utilized the gradient descent back-propagation algorithm to optimize the neurons, while accuracy and loss are among the metrics used to evaluate the performance. From the results, the accuracy of the training process at each epoch was reported in Figure 5, while the loss function was reported in Figure 6.

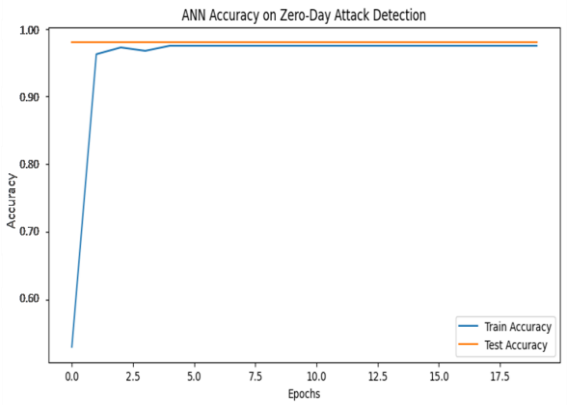

Figure 5: Result of the neural network training process

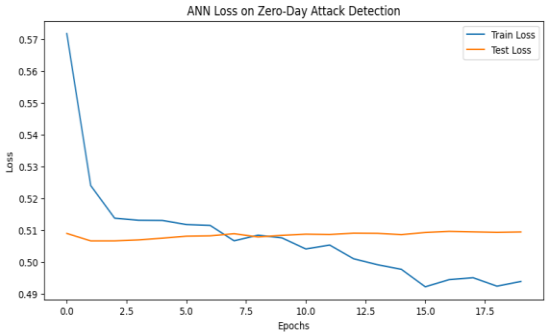

Figure 6: Result of the ANN loss function

Figure 5 reported the accuracy of the training and testing process of the neural network, while considering training loss was reported in Figure 6. From the Figure 5, it was observed that during the training and testing period, the performance of accuracy was very consistent with a high value of 0.985 across different epochs and stops after 18. The loss values in Figure 6 also follow similar patterns for testing performance and overall report a tolerable loss value below 0.51. The results implied that the ANN-based model produced a high success rate in correctly detecting dynamic zero-day attack features. The Figure7 presents a confusion matrix, which measures the model performance in classifying the different classes of threats and normal packets.

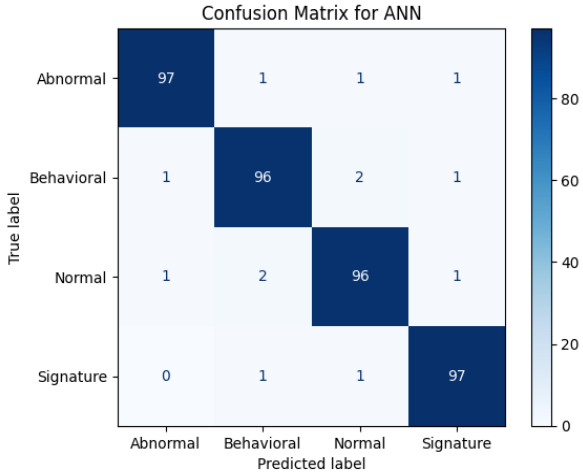

Figure 7: Confusion matrix of the ANN model

Figure 7 presents the confusion matrix of the model considering their True Positive (TP) and False Positive (FP) in correctly classifying the different classes of threat. From the results, it was observed that for anomaly threat, the model recorded 97%. The result also recorded 1% FP for normal, signature, and behavioural threats. For the behavioural class, the model recorded an FP of 1% for anomaly class, and signature class, then 2% FP for normal packets and 96% TR for behavioural analysis classification success. For the classification of normal packets, 1% FP was recorded for anomaly, 2% FP was recorded for behavioural, 96% TP was recorded for normal, and 0% FP was recorded for signature-based class. Signature-based class recorded 1% FP for behavioural and normal packets, while 97% TP was recorded for successful classification of zero-day attacks.

These results implied that the ANN model was able to record high success rate in correctly classifying zero-day attacks. Other metrics like recall, precision, and F1 score were also used to evaluate the model. The precision reported 0.9969, recall recorded 0.9850, and the F1 score recorded 0.9879. These results implied that the model was able to correctly classify zero-day attacks positively with 99%

success, and the recall implied that the model was able to correctly classify zero-day attacksin instances of actual zero-day attacks. The F1score showed that the model succeeded in recording high precision and recall values.

3.1 Result Of System Integration

The system integration discussed the new model for zero-day attack detection, selected with ANN into the 5G cloud network. This was achieved with the Python programming language using data collection from the Litcoder network. Metrics such as detection time, throughput, latency, and CPU utilization were applied to evaluate the model. Figure 8 presents the detection rate of the model after simulation for 20min, with attack injection every 2.5min.

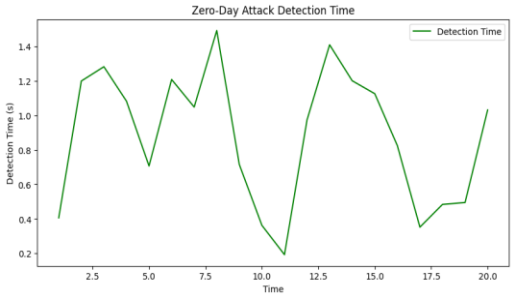

Figure 8: Zero-day attack detection time

The Figure8 measures the average time it takes to detect a zero-day attack. From the results, it was observed that on average, it takes 0.8s to detect a threat on the network. This quick detection time is crucial for real-time security applications, as it minimizes the window of opportunity for an attacker to exploit vulnerabilities. A detection time of 0.8 seconds suggests that the system is highly responsive and capable of identifying and classifying threats swiftly, which is essential for mitigating potential damage and enabling immediate countermeasures. This low detection time indicates that the models are optimized for fast processing, ensuring efficient protection of the network against zero-day attacks. In the next results, the throughput, CPU utilization factor, and latency were evaluated. Table 1 presents the result of system integration.

Table 1: The result of the system Integration

Time (min)	Data Upload (Mbps)	CPU Utilization Factor	Throughput (%)	Latency (ms)
1:00:00	451.8973	0.141306	93.11871	6.564
2:00:00	489.9185	0.178436	92.93143	8.7824
3:00:00	516.0407	0.203946	92.12809	9.0296
4:00:00	527.2945	0.214936	91.28616	9.3336
5:00:00	545.4397	0.232656	90.73143	9.7128
6:00:00	562.1514	0.248976	90.44454	10.604
7:00:00	600.6026	0.286526	90.13113	12.2096
8:00:00	620.7652	0.306216	89.28496	12.2352
9:00:00	642.8631	0.327796	88.99493	13.2064
10:00:00	659.0525	0.343606	87.66522	13.7104
11:00:00	685.7073	0.369636	86.42928	13.9664
12:00:00	691.2164	0.375016	86.21638	14.4128
13:00:00	700.1457	0.383736	85.61215	14.852
14:00:00	720.4311	0.403546	85.48693	16.5128
15:00:00	732.074	0.414916	85.32105	16.832
16:00:00	760.9508	0.443116	85.17853	17.3984
17:00:00	781.3284	0.463016	84.83577	17.4128
18:00:00	785.834	0.467416	84.5882	18.1736
19:00:00	793.514	0.474916	84.46019	20.364
20:00:00	797.5076	0.478816	84.16065	20.6696
Average	720.0299	0.403154	85.09877	27.06957

Table 1 presents the result of the system integration, which occurred by integrating the zero-day attack detection model on the 5G cloud-based network and then evaluate its effectiveness during zero-day attack. Table 1 presents the results of the integrated security model for zero-day attack detection on the 5G cloud network when tested with the injection of simulated zero-day attack feature. The zero-day threat data and also normal data were uploaded on the network. From the results, the CPU utilization factor recorded an average of 0.40315 which is low and showed that the threat features were not allowed throughput to the server. Low CPU utilization indicated less stress on the server and showed that the server had not been overwhelmed with threat. The throughput result recorded very high values averaging 85%. This implied that the threat data was not able to interrupt normal packet flow on the cloud network, since it was intercepted and isolated from the network. Latency was also measured with an average of 27ms. This value is low and very good. What it implies is

that the threat due to its detection and isolation from the network was not able to impact network quality.

CONCLUSION

This study developed and evaluated an improved machine learning-based system applied for dynamic zero-day attack detection and response in 5G cloud-based networks. In the study, by integrating a classification module based on ANN with a real-time threat isolation mechanism, the proposed model demonstrated significant improvements in detection accuracy, response time, and resource efficiency compared to traditional static approaches applied in the previous studies. The ANN model exhibited high classification precision of 0.9969, recall of 0.9850 and F1-score of 0.9879, with a consistent detection performance validated through confusion matrix analysis and simulation. Furthermore, the system was able to detect zero-day threats within 0.8 seconds on average, illustrating its suitability for real-time cybersecurity applications in dynamic network environments.

The system integration results demonstrated in the work further validated the model's practical applicability as it maintained high throughput (average 85.10%), low CPU utilization (0.403) and minimal latency (27.07ms) throughout the simulation. These metrics confirmed the system's ability to detect and isolate malicious traffic without compromising network performance or overburdening computational resources. Overall, the proposed ANN-driven security framework proves to be a robust and adaptive solution for managing zero-day attacks in modern cloud-based 5G infrastructures which offers a proactive and intelligent defence mechanism capable of protecting critical systems against evolving cyber threats while maintaining service quality and performance integrity.

REFERENCES

[1] Aljuaid, W. H., & Alshamrani, S. S. (2024). A deep learning approach for intrusion detection systems in cloud computing environments. *Applied Sciences, 14*(13), 5381. https://doi.org/10.3390/app14135381

[2] amv42. (2018). *sshd-honeypot* (Version 1.0) [Computer software]. GitHub. https://github.com/amv42/sshd-honeypot

[3] Deri, L., & Fusco, F. (2021). Using deep packet inspection in cyber-traffic analysis. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 89–94). IEEE. https://doi.org/10.1109/CSR50904.2021.00021

[4] Dwivedi, R. K., Saran, M., & Kumar, R. (2019). A survey on security over sensor-cloud. In *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 31–37). IEEE. https://doi.org/10.1109/CONFLUENCE.2019.8776897

[5] Erskine, S. K. (2025). Real-time large-scale intrusion detection and prevention system (IDPS) CICIoT dataset traffic assessment based on deep learning. *Applied System Innovation, 8*(2), 52. https://doi.org/10.3390/asi8020052

[6] Harbor M.C, Eneh I.I., Ebere U.C. (2021). Nonlinear dynamic control of autonomous vehicle under slip using improved back-propagation algorithm. International Journal of Research and Innovation in Applied Science (IJRIAS); Vol. 6; Issue 9; https://rsisinternational.org/journals/ijrias/DigitalLibrary/volume-6-issue-9/62-68.pdf

[7] Ilg, N., Duplys, P., Sisejkovic, D., & Menth, M. (2023). A survey of contemporary open-source honeypots, frameworks, and tools. *Journal of Network and Computer Applications, 220*, 103737. https://doi.org/10.1016/j.jnca.2023.103737

[8] Ismail, W. N. (2025). A novel metaheuristic-based methodology for attack detection in wireless communication networks. *Mathematics, 13*(11), 1736. https://doi.org/10.3390/math13111736

[9] Kaur, R., Chana, I., & Bhattacharya, J. (2018). Data deduplication techniques for efficient cloud storage management: A systematic review. *Journal of Supercomputing, 74*(5), 2035–2085. https://doi.org/10.1007/s11227-018-2486-5

[10] Kekong P.E, Ajah I.A., Ebere U.C. (2019). Real-time drowsy driver monitoring and detection system using deep learning based behavioural approach. International Journal of Computer Sciences and Engineering 9 (1), 11-21; http://www.ijcseonline.isroset.org/pub_paper/2-IJCSE-08441-18.pdf

[11] Li, C., Guo, Y., & Wang, X. (2022). Towards privacy-preserving dynamic deep packet inspection over outsourced middleboxes. *High-Confidence Computing, 2*, 100033. https://doi.org/10.1016/j.hicc.2022.100033

[12] Li, M., & Yan, Y. (2024). Comparative analysis of machine-learning models for soil moisture estimation using high-resolution remote-sensing data. *Land, 13*(8), 1331. https://doi.org/10.3390/land13081331

[13] Namasudra, S., Devi, D., Kadry, S., Sundarasekar, R., & Shanthini, A. (2020). Towards DNA based data security in the cloud computing environment. *Computer Communications, 151*, 539–547. https://doi.org/10.1016/j.comcom.2019.12.041

[14] Nkongolo, M., van Deventer, J., & Kasongo, S. M. (2022). Using deep packet inspection data to examine subscribers on the network. *Procedia Computer Science, 215*, 182–191. https://doi.org/10.1016/j.procs.2022.12.021

[15] Nweke, C. I., Ugwu, C. A., Asogwa, M. O., &Kwubeghari, A. U. (2023). Enhancing cyber-security for 5G network: A focus on machine learning-based threat detection. *International Journal of Real-Time Applications and Computing Systems (IJORTACS), 2*(9).

[16] Oduah, U. I., Anierobi, C. M., & Ilori, O. G. (2023). Inventing a robust road-vehicle flood level monitoring device for disaster mitigation. *Heliyon, 9*(10).

[17] Patil, K. (2019). *Securing remote access communications using deep packet inspection* (Master's thesis). National College of Ireland. https://norma.ncirl.ie/4175/1/kapilpatil.pdf

[18] Patzke, T. (2022). *Log4Pot: A honeypot for the Log4Shell vulnerability (CVE-2021-44228)*. GitHub. https://github.com/thomaspatzke/Log4Pot

[19] Safdar, S., Ren, M., Chudhery, M. A. Z., Huo, J., Rehman, H. U., & Rafique, R. (2022). Using cloud-based virtual learning environments to mitigate increasing disparity in urban-rural academic competence. *Technological Forecasting and Social Change, 176*, 121468.

[20] Sarikaya, R., & Hinton, G. E. (2019). A survey of deep learning architectures and their applications. *IEEE Signal Processing Magazine, 23*(4), 11–26. https://doi.org/10.1109/MSP.2019.2900050

[21] Sochima V.E. Asogwa T.C., Lois O.N. Onuigbo C.M., Frank E.O., Ozor G.O., Ebere U.C. (2025)"; Comparing multi-control algorithms for complex nonlinear system: An embedded programmable logic control application; DOI: http://doi.org/10.11591/ijpeds.v16.i1.pp212-224

[22] Talpur, F., Korejo, I. A., Chandio, A. A., Ghulam, A., & Talpur, M. S. H. (2024). ML-based detection of DDoS attacks using EVolutionary Algorithms optimization. *Sensors, 24*(5), 1672.

[23] Tu, S., Huang, X., Huang, Y., Waqas, M., & Rehman, S. U. (2018). SSLSS: Semi-supervised learning-based steganalysis scheme for instant voice communication network. *IEEE Access, 6*, 66153–66164. https://doi.org/10.1109/ACCESS.2018.2874302

[24] Vetterl, A., & Clayton, R. (2019). Honware: A virtual honeypot framework for capturing CPE and IoT zero days. In *14th Symposium on Electronic Crime Research (eCrime 2019)* (pp. 1–13). IEEE. https://doi.org/10.1109/eCrime47957.2019.9037501