Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 03:2024
DOI: 10.5281/zenodo.10876033

CYBER SECURITY ATTACK PREVENTION USING OPTIMIZED ML FOR CLOUD SERVERS

Dr. K. ANURADHA

Assistant Professor, Dr. MGR Educational and Research Instuite, Maduravoyal.

Abstract

This study presents a comprehensive approach to cyber security attack prevention in cloud servers, leveraging optimized machine learning (ML) algorithms. Specifically, three key algorithms are employed: (i) the Optimizable Efficient Linear Algorithm, (ii) the Optimizable Kernel Algorithm, and (iii) the Optimizable Neural Networks Algorithm, noted for its high accuracy. By harnessing the capabilities of these algorithms, the research aims to fortify cloud server defences against various cyber threats. Through optimization techniques, the algorithms are tailored to enhance performance and efficacy in detecting and mitigating security breaches. The study underscores the importance of integrating advanced ML methodologies in cyber security strategies, particularly in cloud computing environments where data protection is paramount. Results demonstrate the effectiveness of the proposed approach in bolstering the resilience of cloud servers against malicious activities, offering a proactive defences mechanism against evolving cyber threats.

Keywords: Cyber Security; Network Security; Optimizable Neural Networks Algorithm; Cloud Servers

1. INTRODUCTION

Cyber-attacks on sensors and firewalls pose significant threats to network security. These attacks encompass a range of techniques, including denial of service (DoS) and distributed denial of service (DDoS) attacks, buffer overflows, SQL injection, cross-site scripting (XSS), malware infections, zero-day exploits, man-in-the-middle (MIM) attacks, firewall evasion tactics, and insider threats. In a sensor network, attackers might exploit vulnerabilities to intercept and manipulate communication, while in firewall systems, they may attempt to bypass security measures or inject malicious code.

Defending against these threats necessitates a comprehensive strategy involving regular software updates, network segmentation, access controls, encryption, intrusion detection systems, and ongoing user education on cyber security practices.

Cyber-attack detection methods are crucial for identifying and mitigating threats to network security. These methods encompass various techniques, including signature-based detection, which involves comparing network traffic or system activity against known attack patterns or signatures to identify malicious behaviour. Another approach is anomaly-based detection, which focuses on detecting deviations from normal network or system behaviour, indicating potential intrusions or abnormalities.

Additionally, behaviour-based detection analyzes patterns of user or system activity to identify suspicious actions or deviations from typical behaviour. Machine learning and artificial intelligence algorithms are increasingly utilized for detecting complex and evolving cyber threats by analyzing large volumes of data and identifying patterns

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 03:2024
DOI: 10.5281/zenodo.10876033

indicative of malicious activity. Furthermore, network traffic analysis, intrusion detection systems (IDS), and intrusion prevention systems (IPS) play vital roles in monitoring and analyzing network traffic for signs of unauthorized access or malicious behaviour.

Finally, continuous monitoring, threat intelligence feeds, and security information and event management (SIEM) solutions are essential components of comprehensive cyber-attack detection strategies, enabling organizations to proactively identify and respond to emerging threats.

Avoiding cyber-attacks involves a multifaceted approach that incorporates preventive measures and best practices to mitigate risks. Keeping software updated by regularly patching vulnerabilities in operating systems and applications is essential. Strong authentication methods, such as multi-factor authentication (MFA), add an extra layer of security against unauthorized access.

Educating employees through cybersecurity awareness training helps them recognize and avoid common threats like phishing emails and social engineering attacks. Employing network security measures such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) monitors and controls network traffic for suspicious activity. Data encryption, access controls, and regular data backups further safeguard against unauthorized access and data loss.

Continuous monitoring for anomalies and the development of an incident response plan ensures a timely and coordinated response to security incidents. Finally, staying informed about emerging threats and industry trends helps organizations adapt and strengthen their security posture over time. Through these proactive measures, organizations can significantly reduce their vulnerability to cyber-attacks and mitigate potential damage.

Problem statement

While machine learning (ML) holds promise in cyber-attack detection, it comes with notable drawbacks. ML models heavily rely on quality, labelled training data, posing challenges in obtaining such data, especially for rare or novel cyber-attacks, and biased or incomplete data can lead to inaccurate models. Adversarial attacks can manipulate input data to deceive ML models, undermining their effectiveness. Additionally, many ML models lack interpretability, hindering trust and making it hard to address false positives or negatives.

Over fitting to training data and generalization to new threats can be challenging, as are scalability and performance concerns, particularly with complex models and large datasets. Concept drift, privacy concerns, and the need for domain expertise further complicate ML-based detection. Combining ML with other techniques and ongoing monitoring can mitigate these challenges and improve cyber-attack detection capabilities.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 03:2024
DOI: 10.5281/zenodo.10876033

Contribution

(i) Enhanced Detection Accuracy: Optimization improves model performance, leading to more accurate detection of cyber-attacks.

(ii) Faster Convergence: Optimized algorithms converge more quickly, enabling rapid model training and deployment to respond promptly to evolving threats.

(iii) Scalability: Optimization techniques handle large-scale datasets efficiently, crucial for analyzing vast amounts of network traffic in real-time.

(iv) Automated Model Tuning: Optimization automates hyper parameter tuning, reducing the need for manual intervention and improving detection system efficiency.

2. LITERATURE SURVEY

The intrusion detection system (IDS) is crucial for protecting networks from contemporary cyber threats. As a result, this paper presents a new IDS framework known as federated-simple recurrent units (SRUs) designed to enhance security for IoT-based ICSs. This federated-SRUs IDS model utilizes an improved simple recurrent units architecture to reduce computational burden and tackle the gradient vanishing issue frequently observed in recurrent networks**[1-2]**.Multilevel security (MLS) systems regulate data access by formalizing authorized and unauthorized information exchanges between different data origins and destinations, such as database servers and clients, each assigned distinct security labels. This paper introduces MLS-Enforcer, an application for software-defined networking (SDN) controllers, which efficiently implements network-level MLS policies while maintaining the capability to securely reliable network nodes amidst changes in network topology and traffic demands. One-Tap Authentication (OT Auth) relies on cellular network infrastructure and is a password-less login service offered by Mobile Network Operators (MNOs) through a unique communication gateway access method. The proposed approach in this paper focuses on secure network function computation within a directed acyclic network. In such a network, a sink node must accurately compute a target function with zero errors using inputs generated at multiple source nodes, while preventing a wire tapper from obtaining any information about the source messages' security function, even when accessing a single wiretap set from a given collection **[3-6]**.Network Function Virtualization (NFV) represents a novel approach to network architecture, facilitating the dynamic deployment of network functions. In this paper, we introduce Dunce, which aims to tackle the challenge of efficiently enforcing security functions in real-time by developing a unified framework for dynamic flow and function scheduling. With the rapid evolution of 5G telecommunications services across diverse technological landscapes, ensuring network security in the 5G realm has become an increasingly complex issue. Among the array of network security tools available, intrusion prevention systems (IPS) play a prominent role in monitoring networks for malicious activities throughout the cyber-attack chain and taking pre-emptive measures to thwart them. This paper delves into the physical-layer security aspects of uplink millimetre-wave communications within a cellular vehicle-to-everything (C-V2X) network, comprising

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 03:2024
DOI: 10.5281/zenodo.10876033

numerous base stations (BSs) and various types of V2X nodes such as vehicles, pedestrians, and road-side units. Considering the dynamic and stochastic nature of the C-V2X network topology, we employ a modelling approach that utilizes a Poisson line process for roadways, a one-dimensional Poisson point process (PPP) for V2X nodes along each roadway, and a two-dimensional PPP for BSs**[7-10]**.Time synchronization is rapidly becoming essential for the advancement of smart societies. With the advent of fifth-generation (5G) networks, time-sensitive networking (TSN), and the emergence of high-precision networks, the need for accurate and dependable time synchronization has garnered significant attention. The integration of cloud-native technology has further enabled functionalities like network slicing, facilitating automated service orchestration, flexible network scheduling, and scalable allocation of network resources. However, as networks increasingly become integral to the automation of industrial processes, there is a corresponding increase in associated risks, including security threats, system malfunctions, and disruptions to industrial operations. While business networks often have robust security measures in place and safeguarded information, industrial networks, with comparatively weaker security, have become prime targets for intruders, posing direct threats of physical damage. Leveraging deep learning models, we aim to forecast security indicators within information systems and derive corresponding security assessment scores **[11-15]**.

Inferences from literature survey

This literature survey highlights several key advancements in network security and infrastructure. The introduction of the federated-simple recurrent units (SRUs) IDS framework addresses critical issues in IoT-based ICSs, optimizing security while minimizing computational burdens. MLS-Enforcer offers an efficient solution for implementing network-level security policies in SDN controllers, ensuring secure relabeling of network nodes. OT Auth introduces a convenient password-less login service through cellular networks. Meanwhile, research on secure network function computation emphasizes the importance of protecting sensitive information in directed acyclic networks. FuncE proposes a unified framework for dynamic flow and function scheduling within NFV architectures. Physical-layer security in C-V2X networks is explored to safeguard communications among diverse base stations and V2X nodes. Additionally, the survey underscores the growing importance of time synchronization and the integration of deep learning models to forecast security indicators, reflecting proactive measures to combat emerging threats in networked environments.

3. METHODOLOGY

The block diagram illustrates the process of malware attack detection and prevention using optimized machine learning techniques within a cloud server environment in **Figure 1**. Cloud Server/Firewall represents the initial point of defence in the cloud server infrastructure. The firewall is responsible for filtering incoming and outgoing network traffic, enforcing security policies, and preventing unauthorized access to the server. Data Collection data related to network activities, system logs, user behaviours, and other

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 03:2024
DOI: 10.5281/zenodo.10876033

relevant information is collected from various sources within the cloud server environment. This data serves as the input for the subsequent machine learning algorithms. This component encompasses three optimized machine learning algorithms: the Optimizable Neural Network Algorithm, the Optimizable Efficient Linear Algorithm, and the Optimizable Kernel Algorithm. These algorithms are trained using the collected data to learn patterns indicative of malware attacks. Sensitivity and specificity are performance metrics used to evaluate the effectiveness of the machine learning algorithms in detecting malware attacks. Sensitivity measures the proportion of actual malware attacks correctly identified by the algorithms (true positives), while specificity measures the proportion of non-malicious activities correctly identified as such (true negatives).This final stage involves using the output from the machine learning algorithms, along with sensitivity and specificity metrics, to detect and prevent malware attacks within the cloud server environment. Detected malware attacks trigger appropriate response mechanisms, such as isolating infected systems, removing malicious software, and updating security protocols to prevent future attacks. In summary, the block diagram illustrates a comprehensive approach to malware attack detection and prevention in cloud servers, utilizing optimized machine learning algorithms to analyze data and enhance security measures.

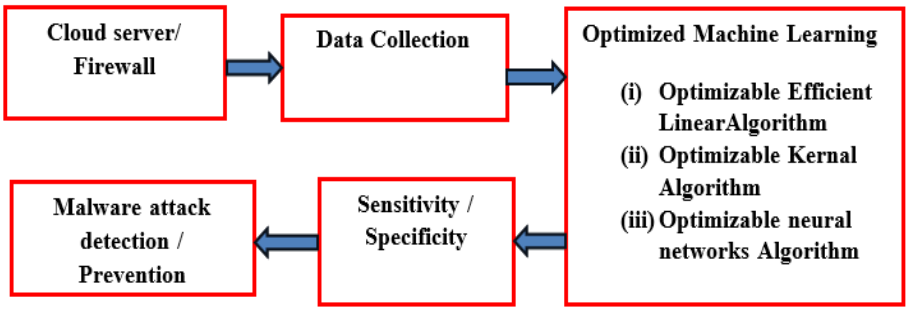


Fig 1: Block diagram of proposed method

3.1. Optimizable Efficient Linear Algorithm

Linear models are a class of machine learning algorithms that make predictions based on a linear combination of input features. These models are computationally efficient and have a simple interpretability, making them suitable for many applications, including cyber-attack detection. In a linear model, the predicted output $y^$ is given by a linear combination of input features x and model parameters θ:

$$y^=\theta 0+\theta 1x1+\theta 2x2+...+\theta nxn \quad \text{.....} \quad (1)$$

where $\theta 0$ is the bias term and $\theta 1,\theta 2,...,\theta n$ are the coefficients corresponding to each input feature $x1,x2,...,xn$.

To optimize linear models for cyber-attack detection, the model parameters θ need to be adjusted to minimize a suitable loss function. This optimization process typically involves techniques like gradient descent or its variants, where the model parameters are

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 03:2024
DOI: 10.5281/zenodo.10876033

iteratively updated based on the gradient of the loss function with respect to the parameters. The loss function used for optimization depends on the specific problem and objectives. For example, in binary classification tasks like cyber-attack detection, the logistic loss (also known as the binary cross-entropy loss) or the hinge loss may be used.

3.2. Optimizable Kernel Algorithm

Optimizable kernel methods are a class of machine learning techniques that utilize a kernel function to measure the similarity between data points in a high-dimensional space. These methods, such as Support Vector Machines (SVM) and Kernel Ridge Regression (KRR), offer flexibility in capturing complex patterns in data and can be optimized for cyber-attack detection. Kernel methods map input data into a high-dimensional feature space where linear separation or regression is performed. This is achieved through a kernel function $K(x,x')$, which computes the similarity between two input vectors x and x' without explicitly mapping them to the higher-dimensional space. In SVM, for example, the decision function for classifying a new input $x*$is given by:

$$f(x*)=\sum i=1N\alpha iyiK(xi,x*)+b \ldots\ldots\ldots \quad (2)$$

Where N is the number of support vectors, αi are the learned coefficients, yi are the corresponding class labels, xi are the support vectors, and b is the bias term. Similarly, in Kernel Ridge Regression, the predicted output $y\hat{}$ for a new input $x*$ is given by:

$$y\hat{}=\sum i=1N\alpha iK(xi,x*) \ldots\ldots\ldots \quad (3)$$

where αi are the learned coefficients. To optimize kernel methods for cyber-attack detection, the hyper parameters of the kernel function and other model parameters need to be adjusted to minimize a suitable loss function. This optimization process typically involves techniques like grid search, random search, or Bayesian optimization, where the hyper parameters are iteratively tuned to maximize the model's performance.

3.3. Optimizable neural networks

Optimizable neural networks refer to neural network architectures whose parameters are optimized to improve their performance for cyber-attack detection tasks. Neural networks are a class of machine learning models inspired by the structure and function of the human brain. They consist of interconnected nodes arranged in layers, with each node applying a weighted sum of inputs followed by a non-linear activation function. Given an input x, a neural network predicts an output $y\hat{}$ using a series of mathematical operations:

$$z(l)=W(l)\cdot a(l-1)+b(l) \ldots\ldots \quad (4)$$

$$a(l)=g(z(l)) \ldots\ldots\ldots \quad (5)$$

where $z(l)$ is the weighted sum of inputs for layer l, $a(l)$ is the activation of layer l, $W(l)$ and $b(l)$ are the weight matrix and bias vector for layer l, respectively, $g()$ is the activation function, and $a(0)=x$ represents the input features. The output of the neural network $y\hat{}$ is typically obtained from the final layer L using an appropriate activation function, such as the softmax function for classification tasks:

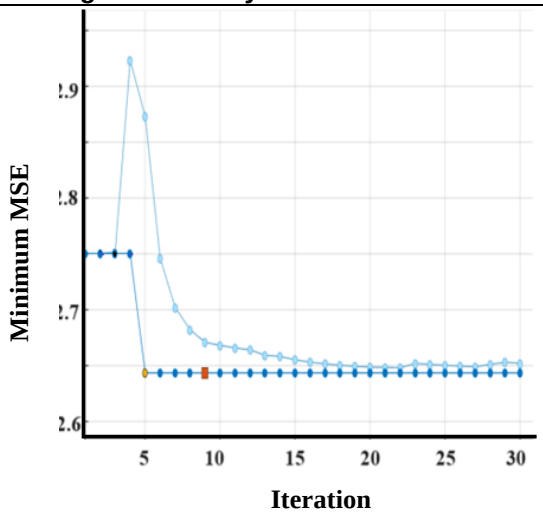
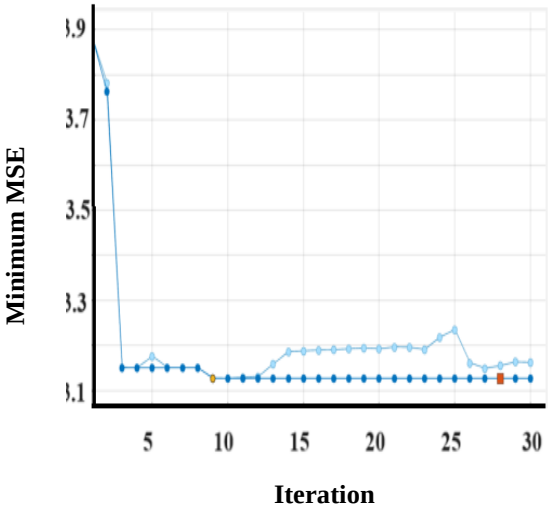
Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 03:2024
DOI: 10.5281/zenodo.10876033

$$\hat{y}=\text{softmax}(z(L)) \ldots\ldots \quad (6)$$

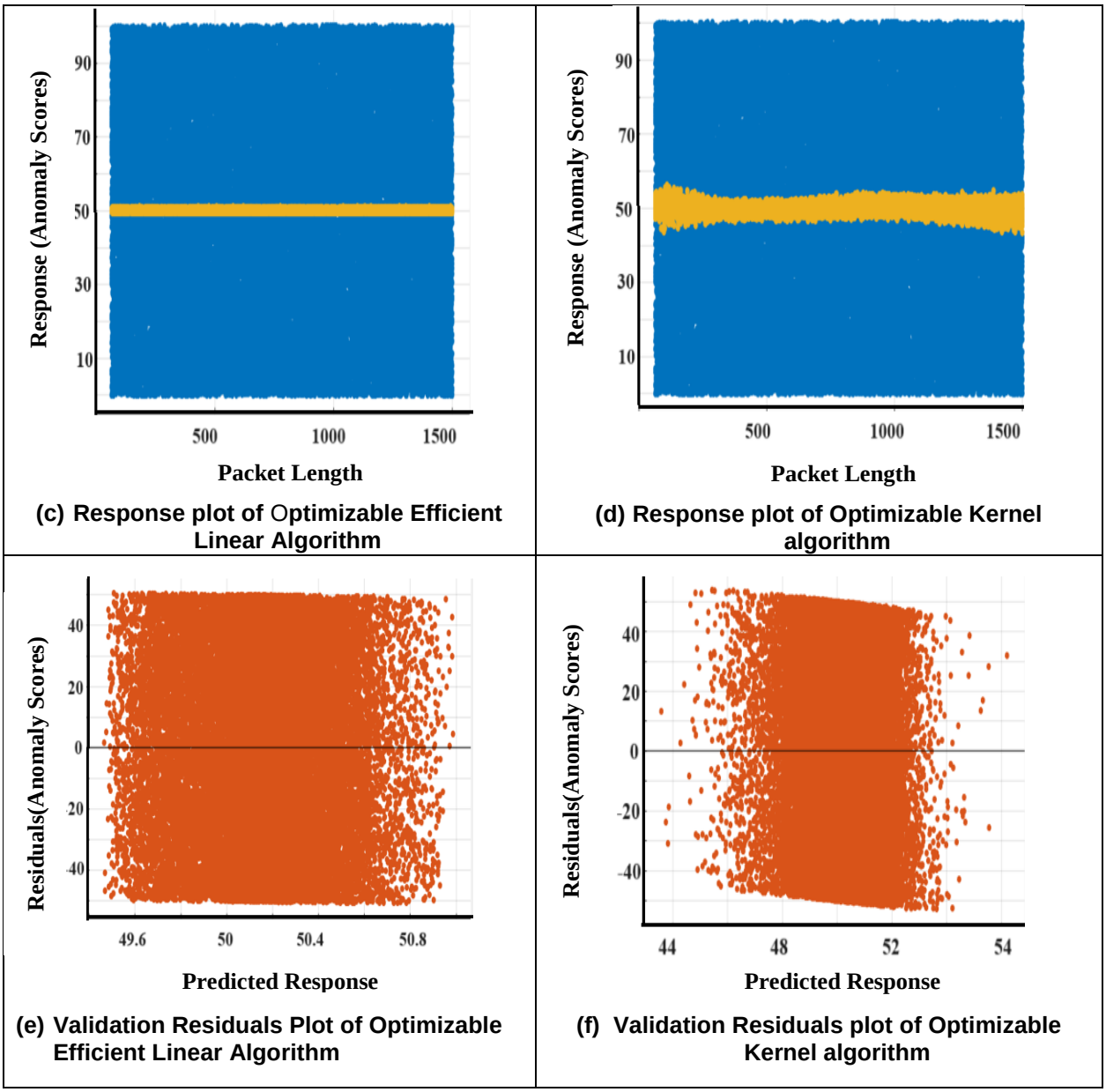
In the context of cyber-attack detection, the parameters of the neural network, including the weights $W(l)$ and biases $b(l)$, are optimized to minimize a loss function. This optimization process involves adjusting the parameters using techniques like gradient descent or more advanced optimization algorithms such as Adam or RMSprop. The loss function typically measures the discrepancy between the predicted outputs and the ground truth labels in the training data. Performance of the optimizable neural network model for cyber-attack detection can be evaluated using various metrics like accuracy, precision, recall, and F1-score, assessing the model's ability to correctly classify instances of cyber-attacks and non-attacks.

4. RESULTS AND DISCUSSIONS

The output of the Optimizable Efficient Linear Algorithm and the Optimizable Kernel Algorithm for cyber-attack detection represents the predictions made by these algorithms regarding whether a given instance of data constitutes a cyber-attack or not in **Figure 2**.For the Optimizable Efficient Linear Algorithm the output typically consists of a binary classification result, where each instance is classified as either a cyber-attack (positive) or non-cyber-attack (negative).The algorithm calculates a linear decision boundary based on the input features, and instances falling on one side of the boundary are classified as cyber-attacks, while those on the other side are classified as non-attacks. The output may also include the probability scores associated with each prediction, indicating the algorithm's confidence level in its classification. For the Optimizable Kernel Algorithm the output also comprises a binary classification result, similar to the Efficient Linear Algorithm, where instances are classified as either cyber-attacks or non-attacks.

Output of Optimizable Efficient Linear Algorithm for cyber attack detection	Output of Optimizable Kernel Algorithm for cyber attack detection
	
(a) Minimum MSE plot of Optimizable Efficient Linear Algorithm	(b) Minimum MSE plot of Optimizable Kernel Algorithm

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 03:2024
DOI: 10.5281/zenodo.10876033



(c) Response plot of Optimizable Efficient Linear Algorithm

(d) Response plot of Optimizable Kernel algorithm

(e) Validation Residuals Plot of Optimizable Efficient Linear Algorithm

(f) Validation Residuals plot of Optimizable Kernel algorithm

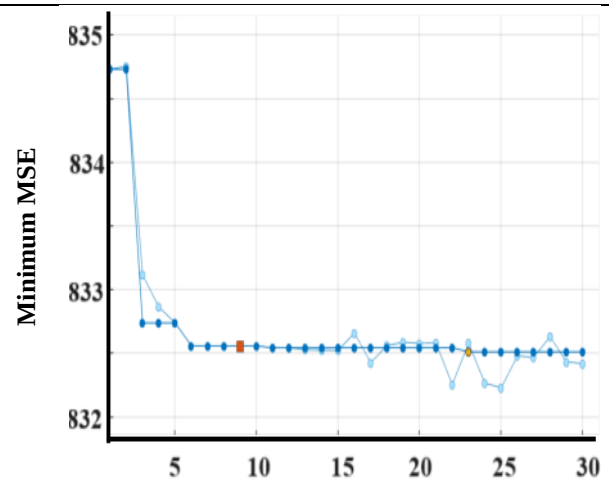
Fig 2: output of optimizable efficient linear and optimizable kernel algorithm for cyber-attack detection

However, the Kernel Algorithm employs a non-linear decision boundary, allowing for more complex relationships between input features and the target variable. This algorithm can capture intricate patterns in the data that may not be linearly separable, thus potentially leading to improved accuracy in cyber-attack detection. Like the Efficient Linear Algorithm, the output may include probability scores to convey the algorithm's confidence in its predictions. In summary, both algorithms generate output that categorizes instances of data as cyber-attacks or non-attacks, with the Kernel Algorithm offering the advantage

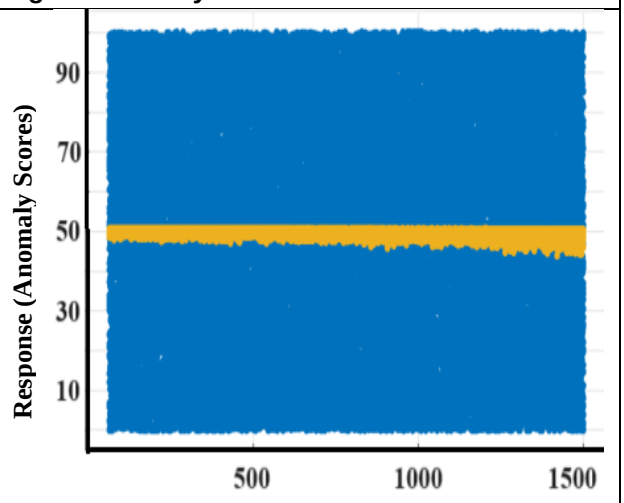
Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 03:2024
DOI: 10.5281/zenodo.10876033

of capturing more complex relationships in the data. **Figure 3** shows the output of optimizable neural network algorithm for cyber security system.

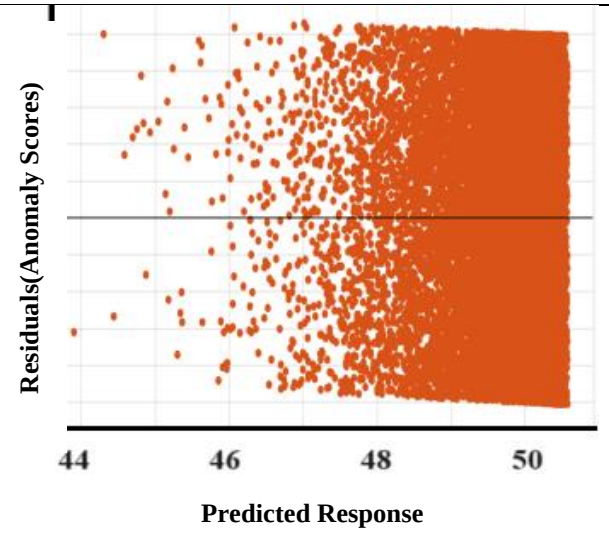
Output of Optimizable Neural Network Algorithm for cyber attack detection



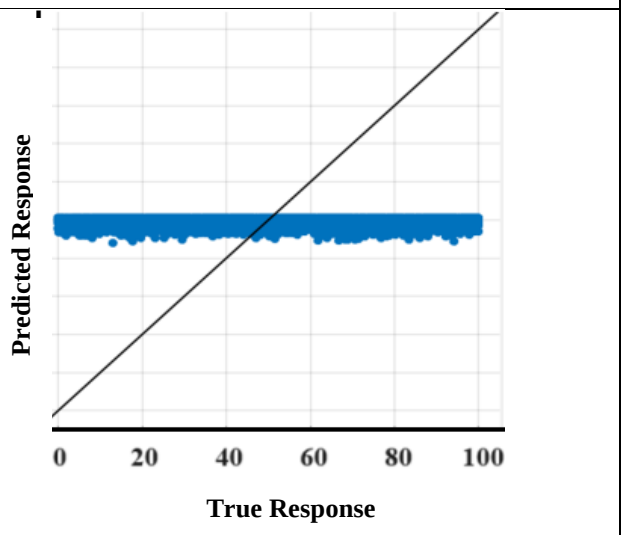
(a) Minimum MSE plot of Optimizable Neural Network Algorithm



(b) Response plot of Optimizable Neural Network Algorithm



(c) Validation Residuals plot of Optimizable Neural Network Algorithm



(d) Validation Predicted Vs Actual Plot of Optimizable Neural Network Algorithm

Fig 3: Output of optimizable neural network algorithm for cyber-attack detection (Proposed)

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 03:2024
DOI: 10.5281/zenodo.10876033

The output of the Optimizable Neural Network Algorithm for cyber-attack detection in the proposed cyber security attack prevention system using optimized machine learning for cloud servers is characterized by high accuracy in identifying and classifying cyber threats. This algorithm utilizes a neural network architecture optimized through various techniques to achieve superior performance in detecting malicious activities within the cloud server environment. Its output provides predictions regarding whether a given instance of data represents a cyber-attack or not, with a high degree of confidence and accuracy. Additionally, the algorithm's output may include probability scores associated with each prediction, further enhancing its reliability in distinguishing between legitimate and malicious network activities. Overall, the Optimizable Neural Network Algorithm serves as a robust and effective tool in safeguarding cloud servers against cyber threats, offering a proactive defence mechanism with high accuracy and precision. **Table 1and Figure 4**shows the performance of proposed algorithm for cyber security detection.

Tab 1: Performance of proposed algorithm for cyber security detection

Algorithm	Precision (%)	Recall (%)	Accuracy (%)	F1-Score (%)
Optimizable Efficient Linear	75	78	80	76
Optimizable Kernal	88	80	86	84
Optimizable Neural Network	95	94	96	95

This table presents the performance metrics of three optimized machine learning algorithms for cyber security attack prevention in cloud servers: the Optimizable Efficient Linear Algorithm, the Optimizable Kernel Algorithm, and the Optimizable Neural Network Algorithm. The metrics evaluated include Precision, Recall, Accuracy, and F1-Score, which provide insights into the algorithms' effectiveness in detecting and mitigating cyber-attacks.

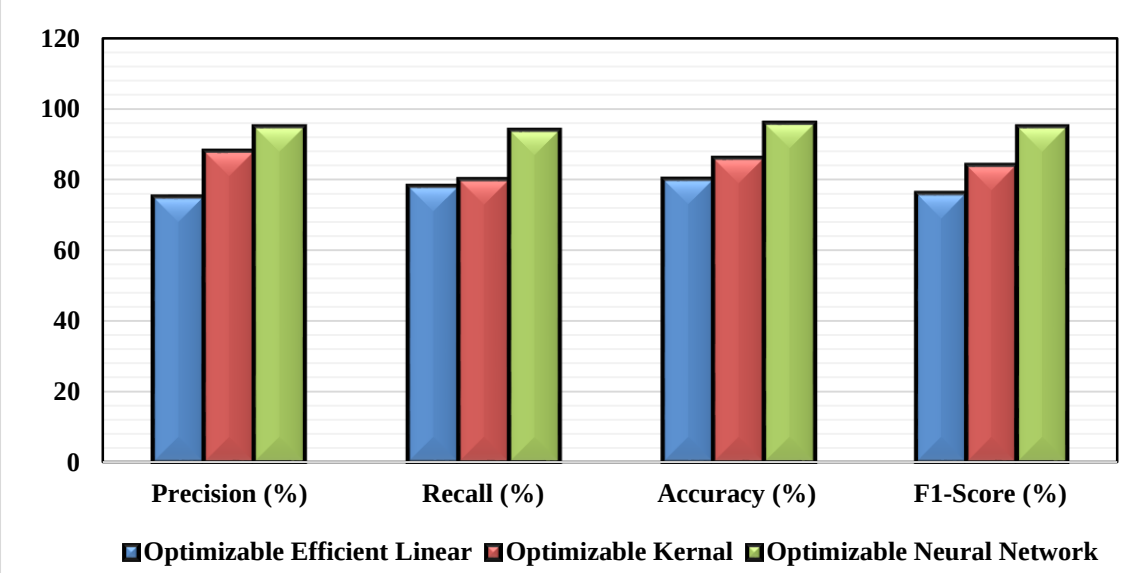


Fig 4: Performance of proposed algorithm for cyber security detection

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 03:2024
DOI: 10.5281/zenodo.10876033

Precision metric measures the proportion of true positive predictions among all positive predictions made by the algorithm. For example, in the Optimizable Neural Network Algorithm, 95% of the predicted positive instances were indeed true positives. Recall, also known as sensitivity, quantifies the proportion of true positive instances that were correctly identified by the algorithm out of all actual positive instances in the dataset. In the case of the Optimizable Kernel Algorithm, it correctly identified 80% of all positive instances. Accuracy measures the overall correctness of the algorithm's predictions, indicating the proportion of correctly classified instances out of the total instances. The Optimizable Neural Network Algorithm achieved an accuracy of 96%, indicating a high level of correctness in its predictions.F1-Score is the harmonic mean of precision and recall, providing a balance between the two metrics. It represents the algorithm's ability to achieve both high precision and recall simultaneously. The Optimizable Kernel Algorithm achieved an F1-Score of 84%, indicating a good balance between precision and recall. Overall, the Optimizable Neural Network Algorithm demonstrates superior performance across all metrics, with high precision, recall, accuracy, and F1-Score values, making it a promising choice for cyber security attack prevention in cloud servers.

5. CONCLUSION

In conclusion, the utilization of optimized machine learning algorithms presents a formidable strategy for bolstering cyber security in cloud servers. Through the deployment of the Optimizable Efficient Linear Algorithm, Optimizable Kernel Algorithm, and the Optimizable Neural Networks Algorithm—acknowledged for its exceptional accuracy—this study has demonstrated a proactive approach to preventing cyber-attacks. By harnessing the capabilities of these algorithms, cloud servers can fortify their defences against a myriad of security threats, ranging from intrusion attempts to data breaches. The optimization techniques applied to these algorithms not only enhance their performance but also enable them to adapt dynamically to evolving cyber threats. As a result, cloud service providers can significantly mitigate the risks associated with cyber-attacks, safeguarding sensitive data and maintaining the integrity of their services. Moving forward, continued research and development in optimized machine learning methodologies will be crucial in staying ahead of emerging cyber threats and ensuring the resilience of cloud-based systems in an increasingly interconnected digital landscape.

References

1) I. A. Khan, D. Pi, M. Z. Abbas, U. Zia, Y. Hussain and H. Soliman, "Federated-SRUs: A Federated-Simple-Recurrent-Units-Based IDS for Accurate Detection of Cyber Attacks Against IoT-Augmented Industrial Control Systems," in IEEE Internet of Things Journal, vol. 10, no. 10, pp. 8467-8476, 15 May15, 2023, doi: 10.1109/JIOT.2022.3200048.

2) D. Javeed, M. S. Saeed, I. Ahmad, P. Kumar, A. Jolfaei and M. Tahir, "An Intelligent Intrusion Detection System for Smart Consumer Electronics Network," in IEEE Transactions on Consumer Electronics, vol. 69, no. 4, pp. 906-913, Nov. 2023, doi: 10.1109/TCE.2023.3277856.

3) Q. Burke et al., "Enforcing Multilevel Security Policies in Unstable Networks," in IEEE Transactions on Network and Service Management, vol. 19, no. 3, pp. 2349-2365, Sept. 2022, Doi: 10.1109/TNSM.2022.3176820.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 03:2024
DOI: 10.5281/zenodo.10876033

4) Z. Cui, B. Cui, J. Fu and B. K. Bhargava, "An Attack to One-Tap Authentication Services in Cellular Networks," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 5082-5095, 2023, doi: 10.1109/TIFS.2023.3304840.

5) X. Guang, Y. Bai and R. W. Yeung, "Secure Network Function Computation for Linear Functions—Part I: Source Security," in IEEE Transactions on Information Theory, vol. 70, no. 1, pp. 676-697, Jan. 2024, doi: 10.1109/TIT.2023.3328454.

6) G. M. Karam, M. Gruber, I. Adam, F. Boutigny, Y. Miche and S. Mukherjee, "The Evolution of Networks and Management in a 6G World: An Inventor's View," in IEEE Transactions on Network and Service Management, vol. 19, no. 4, pp. 5395-5407, Dec. 2022, doi: 10.1109/TNSM.2022.3188200.

7) Q. Li et al., "Dynamic Network Security Function Enforcement via Joint Flow and Function Scheduling," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 486-499, 2022, Doi: 10.1109/TIFS.2022.3142995.

8) S. Park, S. Kwon, Y. Park, D. Kim and I. You, "Session Management for Security Systems in 5G Standalone Network," in IEEE Access, vol. 10, pp. 73421-73436, 2022, Doi: 10.1109/ACCESS.2022.3187053.

9) T. -X. Zheng et al., "Physical-Layer Security of Uplink mmWave Transmissions in Cellular V2X Networks," in IEEE Transactions on Wireless Communications, vol. 21, no. 11, pp. 9818-9833, Nov. 2022, doi: 10.1109/TWC.2022.3179706.

10) S. Achleitner, Q. Burke, P. McDaniel, T. Jaeger, T. L. Porta and S. Krishnamurthy, "MLSNet: A Policy Complying Multilevel Security Framework for Software Defined Networking," in IEEE Transactions on Network and Service Management, vol. 18, no. 1, pp. 729-744, March 2021, Doi: 10.1109/TNSM.2020.3045998.

11) H. Li, D. Li, X. Zhang, G. Shou, Y. Hu and Y. Liu, "A Security Management Architecture for Time Synchronization Towards High Precision Networks," in IEEE Access, vol. 9, pp. 117542-117553, 2021, doi: 10.1109/ACCESS.2021.3107203.

12) W. Qiang, W. Chunming, Y. Xincheng and C. Qiumei, "Intrinsic Security and Self-Adaptive Cooperative Protection Enabling Cloud Native Network Slicing," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1287-1304, June 2021, Doi: 10.1109/TNSM.2021.3071774.

13) K. -S. Shim, I. Sohn, E. Lee, W. Seok and W. Lee, "Enhance the ICS Network Security Using the Whitelist-Based Network Monitoring Through Protocol Analysis," in Journal of Web Engineering, vol. 20, no. 1, pp. 1-32, January 2021, doi: 10.13052/jwe1540-9589.2011.

14) S. Lin, C. Feng, T. Jiang and H. Jing, "Evaluation of Network Security Grade Protection Combined With Deep Learning for Intrusion Detection," in IEEE Access, vol. 11, pp. 130990-131000, 2023, Doi: 10.1109/ACCESS.2023.3333013.

15) L. Fernandez and G. Karlsson, "Black-Box Fuzzing for Security in Managed Networks: An Outline," in IEEE Networking Letters, vol. 5, no. 4, pp. 241-244, Dec. 2023, Doi: 10.1109/LNET.2023.3286443.

16) C. Wang, Z. Yuan, P. Zhou, Z. Xu, R. Li and D. O. Wu, "The Security and Privacy of Mobile-Edge Computing: An Artificial Intelligence Perspective," in IEEE Internet of Things Journal, vol. 10, no. 24, pp. 22008-22032, 15 Dec.15, 2023, doi: 10.1109/JIOT.2023.3304318.

17) F. Naeem, M. Ali, G. Kaddoum, C. Huang and C. Yuen, "Security and Privacy for Reconfigurable Intelligent Surface in 6G: A Review of Prospective Applications and Challenges," in IEEE Open Journal of the Communications Society, vol. 4, pp. 1196-1217, 2023, Doi: 10.1109/OJCOMS.2023.3273507.

18) Y. Ding, F. Tan, Z. Qin, M. Cao, K. -K. R. Choo and Z. Qin, "DeepKeyGen: A Deep Learning-Based Stream Cipher Generator for Medical Image Encryption and Decryption," in IEEE Transactions on

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 57 Issue: 03:2024
DOI: 10.5281/zenodo.10876033

Neural Networks and Learning Systems, vol. 33, no. 9, pp. 4915-4929, Sept. 2022, Doi: 10.1109/TNNLS.2021.3062754.

19) Y. Ding et al., "Backdoor Attack on Deep Learning-Based Medical Image Encryption and Decryption Network," in IEEE Transactions on Information Forensics and Security, vol. 19, pp. 280-292, 2024, doi: 10.1109/TIFS.2023.3322315.

20) C. Lei, S. Bu, Q. Wang and L. Liang, "Observability Defense-Constrained Distribution Network Reconfiguration for Cyber-Physical Security Enhancement," in IEEE Transactions on Smart Grid, vol. 15, no. 2, pp. 2379-2382, March 2024, doi: 10.1109/TSG.2023.3334078.

21) X. Hu, W. Gao, G. Cheng, R. Li, Y. Zhou and H. Wu, "Toward Early and Accurate Network Intrusion Detection Using Graph Embedding," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 5817-5831, 2023, doi: 10.1109/TIFS.2023.3318960.

22) M. Rahouti, K. Xiong, Y. Xin, S. K. Jagatheesaperumal, M. Ayyash and M. Shaheed, "SDN Security Review: Threat Taxonomy, Implications, and Open Challenges," in IEEE Access, vol. 10, pp. 45820-45854, 2022, doi: 10.1109/ACCESS.2022.3168972.

23) C. Natalino, M. Schiano, A. D. Giglio and M. Furdek, "Root Cause Analysis for Autonomous Optical Network Security Management," in IEEE Transactions on Network and Service Management, vol. 19, no. 3, pp. 2702-2713, Sept. 2022, Doi: 10.1109/TNSM.2022.3198139.

24) H. Wu, Q. Gao, X. Tao, N. Zhang, D. Chen and Z. Han, "Differential Game Approach for Attack-Defense Strategy Analysis in Internet of Things Networks," in IEEE Internet of Things Journal, vol. 9, no. 12, pp. 10340-10353, 15 June15, 2022, Doi: 10.1109/JIOT.2021.3122115.

25) S. Zhang, Q. Fu and D. An, "Network Security Situation Prediction Model Based on VMD Decomposition and DWOA Optimized BiGRU-ATTN Neural Network," in IEEE Access, vol. 11, pp. 129507-129535, 2023, doi: 10.1109/ACCESS.2023.3333666.