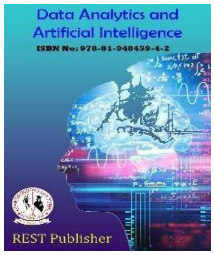
Data Analytics and Artificial Intelligence
Vol: 5(2), 2025
REST Publisher; ISBN: 978-81-948459-4-2
Website: http://restpublisher.com/book-series/daai/
DOI: https://doi.org/10.46632/daai/5/2/5



Decision Tree Regression for Cybersecurity Threat Score Prediction: A Network Behavioral Analysis Using Machine Learning

Rishith Chinthamani
Software Engineer, Walmart, United States.
Corresponding Author Email: rishithchinthamani1@gmail.com

Abstract: *The increasing sophistication of cyber threats necessitates advanced detection mechanisms beyond traditional signature-based approaches. This study investigates the application of Decision Tree Regression for predicting continuous threat scores in cybersecurity environments using network behavioral features. A dataset of 300 observations was analyzed, incorporating packet rate (pkts per sec), average packet size (bytes), failed login count, and threat score as key variables. Descriptive statistics revealed mean packet rates of 201.23 packets/second and average packet sizes of 793.55 bytes, with failed login attempts averaging 0.83 per session. Correlation analysis identified failed login count as the strongest predictor of threat severity ($r = 0.81$), followed by packet rate ($r = 0.45$). The Decision Tree Regression model demonstrated perfect performance on training data ($R^2 = 1.0000$, RMSE = 0.0000), indicating complete pattern memorization. However, testing data evaluation revealed substantial overfitting, with performance declining to $R^2 = 0.8689$, RMSE = 0.0791, and MAE = 0.0663. Despite this degradation, the model maintained reasonable generalization capability, explaining approximately 87% of variance in unseen data. Maximum prediction errors reached 0.1896, highlighting occasional significant deviations from actual threat scores. The findings underscore the critical importance of validating machine learning models on independent test sets to assess true predictive capability. While Decision Tree Regression effectively captures non-linear relationships between network features and threat severity, the substantial performance gap between training and testing phases indicates the need for regularization techniques, ensemble methods, or alternative algorithms to enhance model robustness and reliability in real-world cybersecurity threat detection applications.*

Key Words: *Cybersecurity Threat Detection, Decision Tree Regression, Machine Learning, Network Traffic Analysis, Intrusion Detection.*

1. INTRODUCTION

The growing integration of digital technologies into daily life has significantly elevated the importance of cyber security. This field must contend with a dynamic and ever-evolving threat landscape, where adversaries employ sophisticated methods to exploit vulnerabilities for espionage, disruption, or financial gain. [1] Traditional security measures, such as firewall policies, have become insufficient against modern intrusion techniques that target operating system and network communication weaknesses. In response, the cyber security sector is turning to advanced computational approaches.[2] Research highlights the development of comprehensive, machine learning (ML) frameworks for threat identification in cloud environments, which involve data collection, feature engineering, and model training tailored to cloud-specific challenges.[3] A primary focus of current investigation is the application of deep learning (DL) models, such as Convolution Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), to enhance real-time threat detection and response capabilities. This research explores their strengths and limitations in combating malware, phishing, and insider threats. Furthermore, it addresses critical challenges like adversarial attacks on DL systems and proposes strategies to improve their resilience and interpretability. [4] Concurrently, broader research into Artificial Intelligence (AI) examines its potential to identify complex threats and integrate into existing security architectures. This exploration encompasses not only the operational advantages and disadvantages

Copyright@ REST Publisher

but also the crucial ethical dimensions of deploying AI in cyber security contexts. Together, these efforts aim to revolutionize cyber security practices by combining theoretical insights with practical, AI-driven applications. [5] In the current climate of rapid digital transformation, organizations are increasingly besieged by sophisticated cyber security threats—such as ransom ware, phishing, and insider threats—that jeopardize critical data and disrupt business operations. To counter this, cyber security audits have become indispensable for detecting vulnerabilities, assessing security controls, and ensuring regulatory compliance. [6] A pivotal development in strengthening cyber defenses is the integration of Artificial Intelligence (AI) and Machine Learning (ML). These technologies are revolutionizing threat detection, fraud prevention, and secure data handling across cloud computing, IoT, and financial systems. [7] Recent research underscores this progress, highlighting novel AI-driven models designed for modern challenges. For instance, the MFO-RELM model demonstrates effective threat detection and classification within complex IoT environments. [8] Further qualitative research explores the combined impact of AI and Natural Language Processing (NLP) on cyber security. By analyzing data from diverse sources like social media, healthcare, and finance, and validating findings through expert interviews, studies confirm that AI significantly enhances the ability to identify anomalous patterns in large datasets, a cornerstone of modern threat detection. [9] In conclusion, the evolving threat landscape, which includes supply chain compromises and zero-day exploits, demands that organizations continuously refine their defenses. This requires not only the advancement of detection algorithms but also vigilant monitoring and prompt incident response to stay ahead of malicious actors. [10] Comparative Analysis of ML/DL for Improved Cybersecurity. [11] The primary objective is to address the growing security challenges posed by the widespread adoption of IoT devices and to use these advanced computational methods to detect and classify cyber security threats with high accuracy. The AI Revolution in Cybersecurity Artificial Intelligence (AI) has become a fundamental component of modern cyber security. Its subsets, ML and DL, are crucial for improving threat detection and response algorithms. In particular, supervised learning using labeled datasets is widely used for tasks such as spam filtering, intrusion detection, and malware classification. [12] Limitations of Traditional Methods and the Need for A Traditional cyber security, which relies on signature-based detection and predefined rules, is effective against known threats, but has significant limitations. It struggles to identify new, emerging, or polymorphic attacks that do not match existing signatures. [13] This approach also leads to high false positive rates and requires constant manual updates, which is inadequate against today's sophisticated threat landscape. The Challenge of Evolving Threats and Progressive Learning The relentless evolution of cyber threats demands dynamic and adaptive security solutions. [14] A key challenge and opportunity lies in building models capable of progressive learning. For example, a threat detection model trained on known attack classes (e.g., DDoS, worms) can continuously learn and adapt to identify new attack types (e.g., backdoors, fuzzes), especially in complex environments such as cloud computing where new attack vectors are constantly emerging. In short, the research underscores a critical shift from static, signature-based methods to adaptive, AI-driven architectures that can learn and evolve to address ever-changing cyber threats. [15] The Evolution of Cyber security and Current Challenges Cyber security has undergone significant change over the decades. Initially focused on perimeter security using basic tools such as firewalls and antivirus software, the field has been forced to evolve in response to the expansion of the digital landscape. This growth has been met with increasingly sophisticated attacks, from phishing and malware to state-sponsored cyber operations fueled by geopolitical tensions. [16] The Twin Edges of the AI Revolution While artificial intelligence (AI) and deep learning offer transformative potential for threat detection, they are not a silver bullet. Current AI-powered systems face significant obstacles in achieving the ideal of computationally efficient and accurate real-time, adaptive threat detection. [17] Key challenges include Technical limitations High false positive rates, slow detection speeds, and an inability to identify modern complex threats plague conventional systems. AI models, while advanced, often struggle with adversarial robustness; explain ability, and scalability, preventing their use in large-scale critical infrastructure. [18] The need for human-centric integration: AI cannot operate in a vacuum. Its effectiveness depends on being integrated into a multi-layered security strategy that integrates strong policies, continuous monitoring, and human expertise. [19] Human oversight is critical to interpreting AI insights, fine-tuning models, and responding to sophisticated threats. Furthermore, transparency and explain ability are required to build trust in AI systems, mitigate bias, and ensure stakeholders understand the decision-making process.

2. MATERIALS AND METHODS

Materials

Packet rate pkts per sec: Packet rate pkts per sec represents the number of network packets sent or received by a computer each second, providing a direct measure of traffic intensity. Significant fluctuations in this rate can indicate

unusual activity, such as distributed denial of service (DDoS) attacks, port scanning, malware communication bursts, or sudden spikes caused by unauthorized processes. Monitoring packet rate helps identify performance issues, detect early signs of cyber threats, and assess network stability under different operating conditions.

Average packet size bytes: The Average packet size bytes' value reflects the average size of packets flowing through the network, providing insight into traffic structure and communication behavior. Unusual packet sizes—either very small or unexpectedly large—can suggest malicious activity, such as data exfiltration attempts, command and control communication, probe scans, or fragmented payload delivery. By examining deviations from typical packet-size patterns, security analysts can identify suspicious traffic profiles, detect exploitable vulnerabilities, and better understand emerging cyber threats in real time.

Failed Login Count: Failed Login Count represents the number of failed login attempts recorded within a specified monitoring period. High values may indicate brute force attack attempts, password-guessing activity, credential-stuffing activities, or unauthorized access attempts by internal or external attackers. Monitoring failed logins provides critical insight into account-level security, helps detect compromised credentials, and supports authentication monitoring. Consistent or unusual increases in this count often serve as early warnings of intrusion attempts that require immediate attention from security teams.

Threat Score: Threat Score is a continuous numeric indicator that represents the estimated severity or likelihood of malicious activity, normalized between 0 and 1. This score is derived by combining network behavior metrics such as packet rate, packet size patterns, and failed login attempts. Higher scores indicate stronger evidence of potential threats such as intrusions, malware activity, or data exfiltration. Security systems use this value to prioritize alerts, assess risk levels, and efficiently guide incident response activities.

Decision Tree Regression

Decision Tree Regression is a supervised machine learning algorithm used to predict a series of numerical values by learning simple decision rules from data features. Unlike classification trees, which predict distinct categories, regression trees produce true-valued predictions. The algorithm builds a tree-like model by repeatedly partitioning a dataset into subsets based on feature values. At each node, it selects the feature and range that best minimizes the prediction error, which is typically measured by the mean squared error (MSE) or mean absolute error (MAE). This partitioning process continues until stopping criteria such as maximum depth, minimum samples per leaf, or negligible error reduction are met. To predict a new event, the algorithm traverses the tree from root to leaf, following the branches based on the event's feature values. The leaf node reached determines the predicted output value. Decision tree regression is intuitive, handles nonlinear relationships, requires minimal data preprocessing, and provides feature importance insights. However, it tends to overestimate the training data, producing very complex trees that do not generalize well. Small data variations can significantly change the tree structure, making predictions unstable. To address these limitations, ensemble methods such as Random Forests and Gradient Boosting combine multiple decision trees, improving accuracy and robustness, and reducing overfitting through averaging or boosting techniques.

3. ANALYSIS AND DISCUSSION

The dataset represents network activity patterns used for cybersecurity threat detection, with each record capturing the packet rate, average packet size, failed login attempts, and the associated threat score. The packet rate pkts per sec column shows how actively a system is sending or receiving packets. High values, especially above 300 packets per second, are often associated with high threat scores, reflecting possible scanning or flooding behavior. In contrast, very low packet rates, closer to 1–10, occasionally indicate moderate threat scores, indicating that even minimal network traffic may be suspicious when combined with other factors. Avg packet size bytes varies widely, representing mixed traffic types such as normal browsing, file transfers, or automated scripts. In many rows, even moderate packet rates combined with 1–2 failed logins significantly raise the threat score. The threat score column ranges from 0 to 1, where values above 0.7 indicate highly suspicious activity. The patterns show that high packet bursts, unusual packet sizes, and repeated login failures push the score toward 1, indicating possible attacks such as DDoS attempts, credential stuffing, or espionage.

Copyright@ REST Publisher

TABLE 1. Descriptive Statistics

	Packet Rate Pkts per sec	Avg packet size bytes	Failed login count	Threat score
Count	300	300	300	300
Mean	201.226733	793.5529	0.826667	0.385433
Std	114.004049	288.485168	0.882734	0.200103
Min	1	58.51	0	0
25%	118.0125	588.6775	0	0.243025
50%	207.11	794.375	1	0.3618
75%	275.2	984.9	1	0.498725
Max	662.33	1723.66	4	1

Table 1 summarizes the descriptive statistics of four key variables used in the cybersecurity threat-detection dataset: packet rate, average packet size, failed login count, and threat score. Each variable contains 300 observations, providing a large sample for understanding normal and abnormal network behavior. The packet rate shows a mean of approximately 201 packets per second with a high standard deviation of 114, indicating considerable variation in traffic intensity. The range is quite wide—from a low of 1 packet per second to a high of 662—indicating that the dataset includes both low-activity normal sessions and very high-traffic events that could indicate potential scanning or denial-of-service attempts. Quartile values highlight that typical traffic falls between 118 and 275 packets per second, with a mean close to 207.

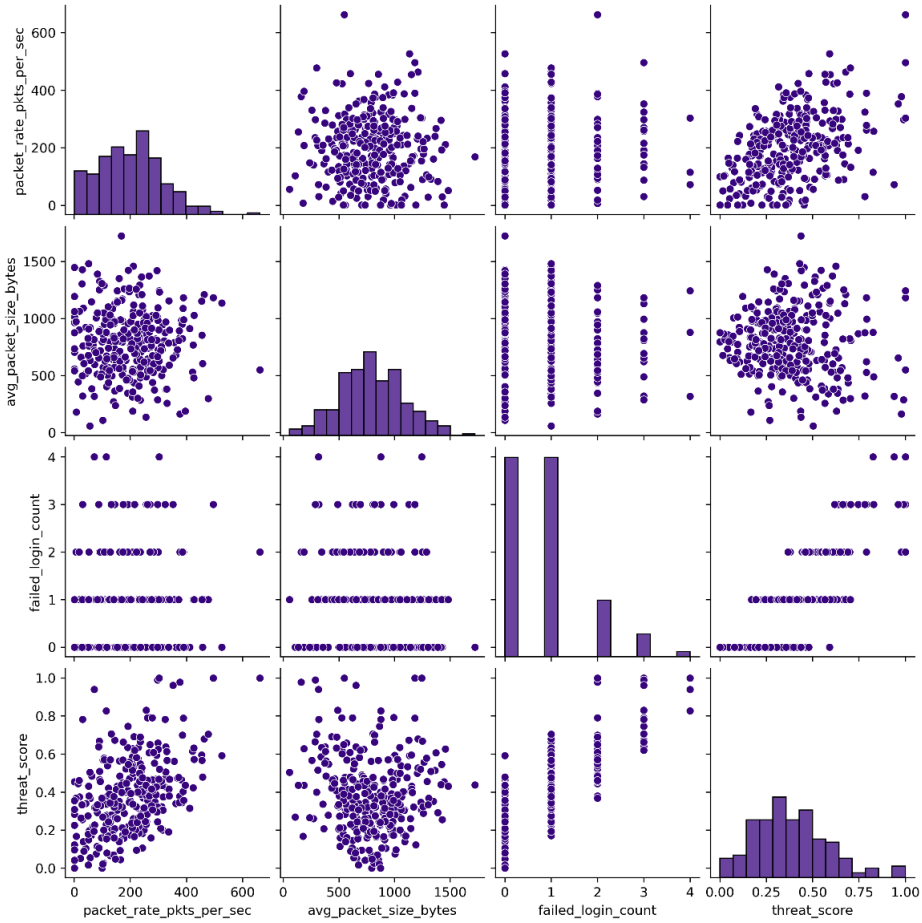


FIGURE 1. Scatter Plot of Various Cybersecurity Threat Detection

Copyright@ REST Publisher

Figure 1 presents a scatter-plot matrix illustrating the relationships between four key variables used in cybersecurity threat detection: packet rate, average packet size, failed login count, and threat score. The diagonal histograms provide a view of the distribution of each variable. The packet rate appears to be skewed to the right, with most observations concentrated between 100 and 300 packets per second, and there are very few extreme high-traffic events above 500. The average packet size shows a very uniform distribution, forming a normal pattern centered around 800–900 bytes. The failed login count is very skewed, dominated by zero and single failed attempts, with relatively few cases showing two or more, indicating that extreme brute force activities are less common. The threat score shows a wide spread from 0 to 1, indicating that the dataset includes both benign and high-risk events. The scatter plots reveal important correlation patterns. Packet rate and threat score show a mild positive relationship – higher packet bursts often correspond to higher threat values, although the relationship is not strictly linear. Packet size similarly shows moderate scatter against threat score, indicating that unusually large packets sometimes correlate with suspicious behavior, but not consistently. A strong visual pattern emerges in the failed login count versus threat score plot: events with multiple failed credentials often cluster in the upper threat range (0.6–1), reinforcing the importance of login attempts as a key indicator of malicious activity.

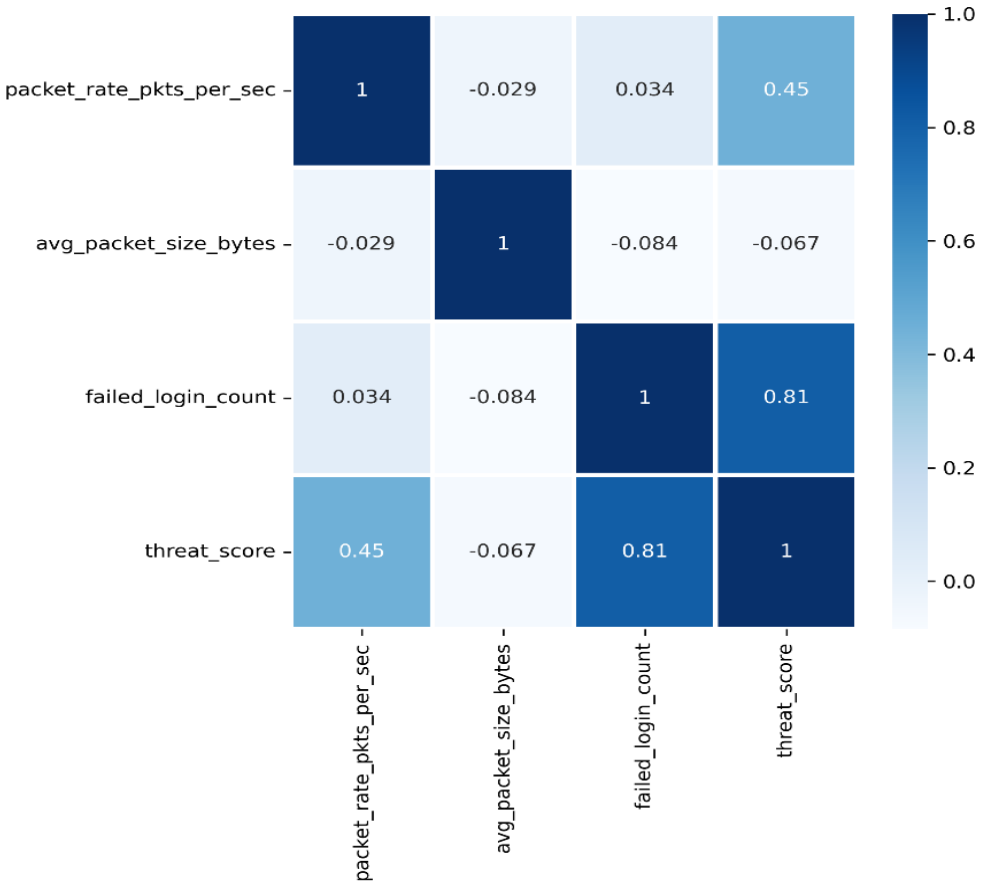


FIGURE 2. Correlation Heat Map Depicting the Relationships Between Process Parameters and Response Variables

Figure 2 presents a correlation heat map that illustrates the strength and direction of the relationships between four cybersecurity threat-detection variables: packet rate, average packet size, failed login count, and threat score. The color gradient ranges from dark blue (strong positive correlation) to lighter shades indicating weak or negative correlations. The heat map provides a brief visual summary of how each parameter contributes to overall threat behavior and how closely they are correlated. The most significant relationship is between failed login count and threat score, which shows a strong positive correlation of 0.81. This indicates that as failed login attempts increase, the threat score increases significantly. This pattern is consistent with typical cybersecurity scenarios, where repeated login

Copyright@ REST Publisher

failures suggest brute force attacks or unauthorized access attempts. The second significant correlation is between packet rate and threat score at 0.45, indicating a moderate positive relationship. High packet rates often occur during suspicious activities such as scanning, flooding, or automated bot traffic, which raises the risk level. Other relationships in the heat map show very weak or negligible correlations. For example, the correlation between average packet size and threat score is slightly negative (–0.067), indicating that packet size alone is not a strong indicator of malicious behavior. Similarly, the correlations between packet rate and packet size (–0.029) and packet size and failed login count (–0.084) do not show a meaningful relationship, reflecting the fact that these variables act independently in most network operations.

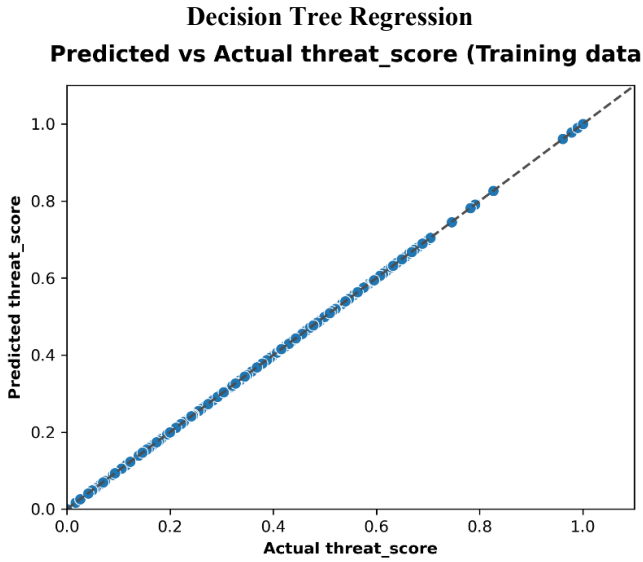


FIGURE 3. Decision Tree Regression (Training data)

Looking at Figure 3, this scatter plot demonstrates the performance of a Decision Tree Regression model on training data. The graph shows predicted threat scores plotted against actual threat scores, with points forming a nearly perfect diagonal line along the dashed reference line. This indicates exceptional model fit, with predictions closely matching actual values across the entire range from 0.0 to 1.0. The tight clustering of data points along the ideal prediction line suggests the model has learned the training patterns extremely well, achieving minimal prediction error.

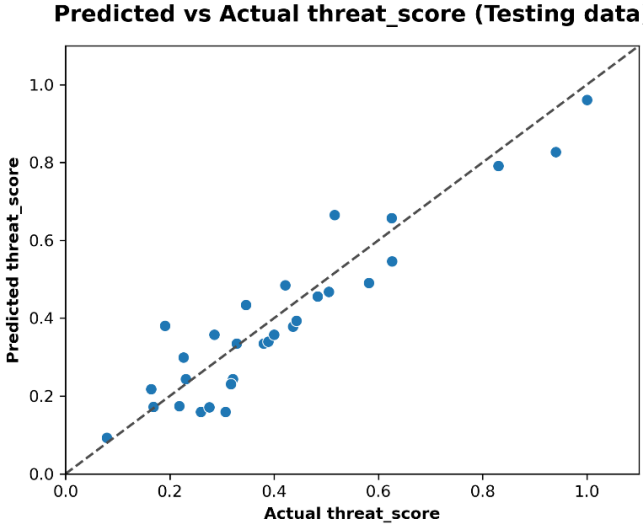


FIGURE 4. Decision Tree Regression (Testing data)

Copyright@ REST Publisher

Looking at Figure 4, this scatter plot displays the Decision Tree Regression model's performance on testing data. The predicted threat scores are plotted against actual threat scores, showing considerably more scatter compared to the training data results. While the points generally follow the diagonal reference line, indicating reasonable predictive capability, there is noticeable deviation from perfect predictions. The spread of points around the ideal line reveals the model's reduced accuracy on unseen data, particularly visible in the mid-range values where some predictions diverge more significantly. This increased variance between predicted and actual scores is typical and healthy, confirming the model generalizes to new data rather than merely memorizing training patterns, though some prediction error remains.

TABLE 2. Decision Tree Regression (Training Data, Testing Data)

Data	R2	EVS	MSE	RMSE	MAE	Max Error	MSLE	Med AE
Train	1.0000	1.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
Test	0.8689	0.8741	0.0062	0.0791	0.0663	0.1896	0.0034	0.0556

Table 2 presents comprehensive performance metrics for the Decision Tree Regression model across training and testing datasets. The training data shows perfect scores across all metrics ($R^2 = 1.0000$, MSE = 0.0000, MAE = 0.0000), confirming complete memorization of training patterns and raising overfitting concerns. In contrast, the testing data reveals the model's true generalization capability with $R^2 = 0.8689$, indicating it explains approximately 87% of variance in unseen data. The testing metrics show RMSE of 0.0791 and MAE of 0.0663, representing acceptable prediction errors. The maximum error of 0.1896 suggests some predictions deviate notably from actual values. The substantial performance gap between training and testing datasets confirms overfitting occurred, though the model still demonstrates reasonable predictive ability on new data, making it potentially useful despite not achieving the perfect training performance.

4. CONCLUSION

This research demonstrates the application of Decision Tree Regression for cybersecurity threat detection, utilizing network behavioral metrics to predict continuous threat scores. The study analyzed 300 observations encompassing packet rate, average packet size, failed login count, and threat score, revealing critical insights into malicious activity patterns. Correlation analysis established failed login count as the most influential predictor ($r = 0.81$), confirming that repeated authentication failures serve as strong indicators of brute force attacks and unauthorized access attempts. Packet rate exhibited moderate correlation ($r = 0.45$) with threat severity, while packet size showed minimal predictive value, suggesting that traffic volume and authentication anomalies are more reliable threat indicators than individual packet dimensions. The Decision Tree Regression model achieved flawless performance on training data, with perfect R^2 scores and zero error metrics across all measures. However, this exceptional performance masked significant overfitting, as evidenced by the substantial degradation observed during testing phase evaluation. The model's testing performance ($R^2 = 0.8689$, RMSE = 0.0791, MAE = 0.0663) revealed that while it retained reasonable generalization capability, explaining approximately 87% of variance in unseen data, the considerable gap between training and testing metrics highlights the algorithm's tendency to memorize rather than learn generalizable patterns. Despite these limitations, the model demonstrates practical utility for threat assessment, maintaining acceptable prediction accuracy on novel data. The maximum error of 0.1896 indicates occasional significant mispredictions that could impact critical security decisions. Future research should explore regularization techniques such as pruning, setting appropriate maximum depth constraints, and minimum sample requirements to mitigate overfitting. Additionally, ensemble methods like Random Forests or Gradient Boosting could enhance prediction stability and robustness. Incorporating additional features such as temporal patterns, protocol types, and geographical indicators may further improve detection accuracy. The integration of human expertise with automated AI-driven threat scoring remains essential for interpreting model outputs and responding effectively to sophisticated cyber threats in dynamic operational environments.

REFERENCE

[1]. Sewak, Mohit, Sanjay K. Sahay, and Hemant Rathore. "Deep reinforcement learning for cybersecurity threat detection and protection: A review." In International Conference on Secure Knowledge Management in Artificial Intelligence Era, pp. 51-72. Cham: Springer International Publishing, 2021.

Copyright@ REST Publisher

[2]. Sornsuwit, Ployphan, and Saichon Jaiyen. "A new hybrid machine learning for cybersecurity threat detection based on adaptive boosting." Applied Artificial Intelligence 33, no. 5 (2019): 462-482.
[3]. Rao, Deepak Dasaratha, Sairam Madasu, Srinivasa Rao Gunturu, Ceres D'britto, and Joel Lopes. "Cybersecurity threat detection using machine learning in cloud-based environments: A comprehensive study." International Journal on Recent and Innovation Trends in Computing and Communication 12, no. 1 (2024): 285-290.
[4]. Okafor, Maureen Oluchukwuamaka. "Deep learning in cybersecurity: Enhancing threat detection and response." World Journal of Advanced Research and Reviews 24, no. 3 (2024): 1116-1132.
[5]. Sunkara, Goutham. "AI Powered Threat Detection in Cybersecurity." International Journal of Humanities and Information Technology Special 1 (2021): 1-22.
[6]. Mohammed, Anwar. "Elevating Cybersecurity Audits: How AI is Shaping Compliance and Threat Detection." Aitoz Multidisciplinary Review 2, no. 1 (2023): 35-43.
[7]. Kumar, Busireddy Hemanth, Sai Teja Nuka, Murali Malempati, Harish Kumar Sriram, Someshwar Mashetty, and Sathya Kannan. "Big Data in Cybersecurity: Enhancing Threat Detection with AI and ML." Metallurgical and Materials Engineering 31, no. 3 (2025): 12-20.
[8]. Alrowais, Fadwa M., Sami Althahabi, Saud S. Alotaibi, Abdullah Mohamed, Manar Ahmed Hamza, and Radwa Marzouk. "Automated Machine Learning Enabled Cybersecurity Threat Detection in Internet of Things Environment." Comput. Syst. Sci. Eng. 45, no. 1 (2023): 687-700.
[9]. Ismail, Walaa Saber. "Threat detection and response using AI and NLP in cybersecurity." J. Internet Serv. Inf. Secur 14, no. 1 (2024): 195-205.
[10]. Manoharan, Ashok, and Mithun Sarker. "Revolutionizing cybersecurity: Unleashing the power of artificial intelligence and machine learning for next-generation threat detection." DOI: https://www. doi. org/10.56726/IRJMETS32644 1 (2023).
[11]. Gopalsamy, Mani. "An Optimal Artificial Intelligence (AI) technique for cybersecurity threat detection in IoT Networks." Int. J. Sci. Res. Arch 7, no. 2 (2022): 661-671.
[12]. Sankaram, Mosa, Ms Roopesh, Sasank Rasetti, and Nourin Nishat. "A comprehensive review of artificial intelligence applications in enhancing cybersecurity threat detection and response mechanisms." Management 3, no. 5 (2024).
[13]. Katiyar, Nirvikar, Mr Somendra Tripathi, Mr Praveen Kumar, Mr Shekhar Verma, Alok Kumar Sahu, and Shailesh Saxena. "AI and Cyber-Security: Enhancing threat detection and response with machine learning." Educational Administration: Theory and Practice 30, no. 4 (2024): 6273-6282.
[14]. Vemuri, Naveen, Naresh Thaneeru, and Venkata Manoj Tatikonda. "Adaptive generative AI for dynamic cybersecurity threat detection in enterprises." International Journal of Science and Research Archive 11, no. 1 (2024): 2259-2265.
[15]. Karn, Rupesh Raj, Prabhakar Kudva, and Ibrahim M. Elfadel. "Learning without forgetting: A new framework for network cyber security threat detection." IEEE Access 9 (2021): 137042-137062.
[16]. Dalal, Aryendra. "Exploring next-generation cybersecurity tools for advanced threat detection and incident response." Available at SSRN 5424096 (2020).
[17]. Khalaf, Noora Zidan, Israa Ibraheem Al Barazanchi, A. D. Radhi, Sushma Parihar, Pritesh Shah, and Ravi Sekhar. "Development of real-time threat detection systems with AI-driven cybersecurity in critical infrastructure." Mesopotamian Journal of CyberSecurity 5, no. 2 (2025): 501-513.
[18]. Polamarasetti, Anand, Rahul Vadisetty, Vasu Velaga, KishanKumar Routhu, Gangadhar Sadaram, Suneel Babu Boppana, and Srikanth Reddy Vangala. "Enhancing Cybersecurity Architectures with Artificial Intelligence (AI): A Framework for Automated Threat Intelligence Detection System." Universal Library of Engineering Technology Issue (2023). Danish, Muhammad. "Enhancing cyber security through predictive analytics: Real-time threat detection and response." arXiv preprint arXiv:2407.10864 (2024).
[19]. Raji, Adeola, Abiola Olawore, Adeyinka Mustapha, and Jennifer Joseph. "Integrating Artificial Intelligence, machine learning, and data analytics in cybersecurity: A holistic approach to advanced threat detection and response." World Journal of Advanced Research and Reviews 20, no. 3 (2023): 2005-2024.
[20]. Hesham, Momen, Mohamed Essam, Mohamed Bahaa, Ahmed Mohamed, Mohamed Gomaa, Mena Hany, and Wael Elsersy. "Evaluating predictive models in cybersecurity: a comparative analysis of machine and deep learning techniques for threat detection." In 2024 Intelligent Methods, Systems, and Applications (IMSA), pp. 33-38. IEEE, 2024.
[21]. Drucker, H., Burges, C. J. C., Kaufman, L., Smola, A., & Vapnik, V. (1997). Support vector regression machines. Advances in Neural Information Processing Systems, 9, 155–161.
[22]. Vapnik, V. N. (1995). The Nature of Statistical Learning Theory. Springer, New York.
[23]. Smola, A. J., & Schölkopf, B. (2004). A tutorial on support vector regression. Statistics and Computing, 14, 199–222.
[24]. Schölkopf, B., & Smola, A. J. (2002). Learning with Kernels: Support Vector Machines, Regularization, Optimization, and Beyond. MIT Press.
[25]. Basak, D., Pal, S., & Patranabis, D. C. (2007). Support vector regression. Neural Information Processing–Letters and Reviews, 11(10), 203–224.

Copyright@ REST Publisher