World Journal of Innovation and Modern Technology, Vol. 7, Issue 6, (Dec) 2024
ISSN 2682-5910
DOI: 10.53469/wjimt.2024.07(06).09

Threat Detection Driven by Artificial Intelligence: Enhancing Cybersecurity with Machine Learning Algorithms

Heyao Chen[1], Zepeng Shen[2], Yong Wang[3], Hu Ke[4], Jian Xu[5]

[1]Computer Science and Technology, Beijing University of Posts and Telecommunications, Beijing, China
[2]Network Engineering, Shaanxi University of Technology, Shaanxi 723001, China
[3]Information Technology, University of Aberdeen, Aberdeen, United Kingdom
[4]Mechanical Design,Manufacturing and Automation,Heilongjiang Institute of Technology,Heilongjiang,China
[5]Electrical and Electronics Engineering,University of Southern California, California, USA

Abstract: ***This paper aims to explore the applications of artificial intelligence (AI) and machine learning (ML) in the field of cybersecurity, particularly in the development of end-to-end solutions for threat detection. By analyzing the current challenges in cybersecurity and the limitations of traditional threat detection methods, this paper seeks to demonstrate how AI/ML technologies can enhance the efficiency, accuracy, and automation levels of threat detection. The paper begins by introducing the core concepts of cybersecurity threat detection, including traditional methods such as signature-based detection, behavior-based detection, and rule-based detection systems. It then elaborates on the applications of machine learning in anomaly detection, malware detection, network traffic analysis, intrusion detection systems (IDS) and intrusion prevention systems (IPS), as well as user behavior analytics (UBA). Following this, the paper discusses the importance of data preprocessing and feature engineering in threat detection and their practical applications, including data cleaning, feature selection, and extraction. Finally, the paper explores the training and evaluation of models, the deployment of models, and the challenges they face, along with future trends in AI-driven threat detection. The research results indicate that AI/ML technologies can significantly improve the accuracy and efficiency of threat detection, particularly in handling unknown threats and automating detection processes. Through the application of various machine learning algorithms, such as anomaly detection, malware detection, and network traffic analysis, systems can better identify and respond to various network threats. However, AI-driven threat detection still faces challenges related to data quality, algorithm performance, and system implementation.***

Keywords: AI; cybersecurity.

1. INTRODUCTION

1.1 Current Status and Challenges of Cybersecurity

1.1.1 Recent Trends in Cyber Threats

In recent years, the landscape of cyber threats has become increasingly severe, with attackers constantly upgrading their tactics. The threats have evolved from traditional viruses and Trojan horses to more sophisticated ransomware, supply chain attacks, and advanced persistent threats (APTs). These threats not only impact personal and enterprise data security but also pose significant challenges to national security. With the widespread adoption of IoT, cloud computing, and 5G technologies, the attack surface has expanded, making defense significantly more difficult[1].

1.1.2 Limitations of Traditional Threat Detection Methods

Traditional threat detection methods primarily rely on rule-based and signature matching. While these methods perform reasonably well against known threats, they are inadequate in dealing with unknown threats. Moreover, these approaches typically require extensive manual intervention and expert knowledge, resulting in low efficiency and high costs. As the complexity and diversity of threats increase, the limitations of traditional methods become more pronounced, necessitating new technological means to address current cybersecurity challenges[2].

2. CORE CONCEPTS OF THREAT DETECTION

2.1 Definition and Importance of Threat Detection

2.1.1 Definition: What is Threat Detection?

Threat detection refers to the process of identifying, analyzing, and responding to potential malicious activities or behaviors in computer systems, networks, and data through a series of technical means and methods. Threat detection not only involves discovering attacks but also includes assessing potential risks and determining whether these risks will evolve into actual attack behaviors. The scope of threat detection is broad, covering traditional malicious software such as viruses, Trojans, and worms, as well as complex attack methods like phishing attacks, denial-of-service attacks (DDoS), and advanced persistent threats (APTs). Through threat detection, security teams can take timely measures to prevent or mitigate the damage caused by attacks. Threat detection is the first line of defense in the cybersecurity defense system, and its importance is self-evident as it directly relates to the security and integrity of systems and data.[5]

2.1.2 Position and Role in the Cybersecurity Defense System

In the cybersecurity defense system, threat detection occupies a core position and is an integral part of the overall security architecture. It not only helps identify potential security threats but also provides critical information for subsequent threat response, risk assessment, and security decision-making. Specifically, threat detection systems typically follow firewalls, intrusion prevention systems (IPS), and data loss prevention systems (DLP) in the security stack, responsible for real-time monitoring of network traffic and system behaviors to detect suspicious activities. By promptly detecting potential threats, security teams can swiftly take measures such as blocking attack sources, isolating infected devices, or initiating emergency response plans. The effectiveness of threat detection directly impacts the overall performance of the cybersecurity defense system, making it a key component in ensuring the security and integrity of systems and data[6].

2.2 Traditional Methods of Threat Detection

2.2.1 Signature-Based Detection Methods

Signature-based detection methods are among the most common in traditional threat detection. This approach relies on a database of known threat signatures, which are unique identifiers of specific threats, akin to the "fingerprints" of viruses. When the detection system identifies activities or behaviors matching these signatures in network traffic or files, it triggers an alert or takes corresponding defense actions. Signature-based methods are highly effective against known threats, as they can quickly identify and block known malware and attack methods. However, their limitations are also apparent: they can only detect known threats and are powerless against unknown threats or variations. Additionally, the signature database requires constant updates to address new threats, leading to high maintenance costs[7].

3. CHAPTER 3: APPLICATION OF MACHINE LEARNING ALGORITHMS IN THREAT DETECTION

3.1 Anomaly Detection

3.1.1 Definition and Characteristics of Anomaly Detection

Anomaly detection refers to the process of identifying abnormal behaviors or activities in systems or networks that significantly deviate from normal patterns, possibly indicating the presence of a potential threat or attack. The core task of anomaly detection is to find points in massive data that significantly deviate from baseline behaviors. It is characterized by not relying on specific attack patterns or features but rather analyzing the statistical properties and patterns of normal behaviors to identify abnormalities. Anomaly detection methods are widely used in network intrusion detection, fraud detection, system monitoring, and other areas, making them an essential component of threat detection[15].

3.1.2 Common Algorithms: K-Means, Isolation Forest, Autoencoder, etc.

Common machine learning algorithms used in anomaly detection include K-Means, Isolation Forest, and Autoencoder. K-Means is a distance-based clustering algorithm that identifies outliers by clustering data points to their nearest centroids. Isolation Forest is an efficient anomaly detection algorithm that isolates outliers by constructing random decision trees, known for its fast computation and effectiveness with high-dimensional data.

Autoencoder is a deep learning algorithm that identifies anomalies by learning compressed representations of data; data points with high reconstruction errors are considered anomalies. Each of these algorithms has its strengths and weaknesses, and the appropriate algorithm can be chosen based on the specific application scenario[16].

3.1.3 Application Case: Detecting Abnormal Traffic and Behaviors

A common application of anomaly detection in threat detection is the identification of abnormal network traffic and user behaviors. By monitoring network traffic and system logs, machine learning algorithms can identify patterns that significantly deviate from normal behaviors, thus discovering potential attacks or security incidents. For example, in an enterprise network, anomaly detection can be used to identify unauthorized access, large-scale data leakage, or abnormal command execution. Additionally, in cloud computing environments, anomaly detection can help identify abnormal behaviors of virtual machines to prevent malware and internal threats. By combining multi-layer anomaly detection methods, a comprehensive threat detection system can be built, enhancing overall cybersecurity defense capabilities[17].

3.2 Malware Detection

3.2.1 Basic Concepts of Malware Detection

Malware detection involves identifying and classifying malicious software using machine learning algorithms, which pose significant threats to systems, networks, and data. Malware covers a wide range of categories, including viruses, worms, Trojans, ransomware, and more. The goal of malware detection is to accurately identify these malicious software and take corresponding defense measures, such as isolation, deletion, or blocking their spread. With the increasing variety and quantity of malware, traditional signature-based and rule-based detection methods are no longer sufficient, and machine learning methods have become an essential means due to their efficiency and flexibility[18].

3.3 Network Traffic Analysis

3.3.1 Importance of Network Traffic Analysis

Network traffic analysis is a critical component of cybersecurity, enabling in-depth analysis of network data to identify potential threats and abnormal behaviors. Its importance lies in several aspects: First, it helps detect unauthorized access and malicious activities such as DDoS attacks, malware dissemination, and data leaks. Second, monitoring and analyzing traffic patterns can identify abnormal behavior within the internal network, preventing insider threats. Additionally, network traffic analysis can also be used for performance optimization and resource management, identifying and optimizing network bottlenecks to improve overall network efficiency. Through real-time and historical traffic analysis, security teams can gain comprehensive cybersecurity situational awareness, responding promptly to potential threats and protecting network and data security[22].

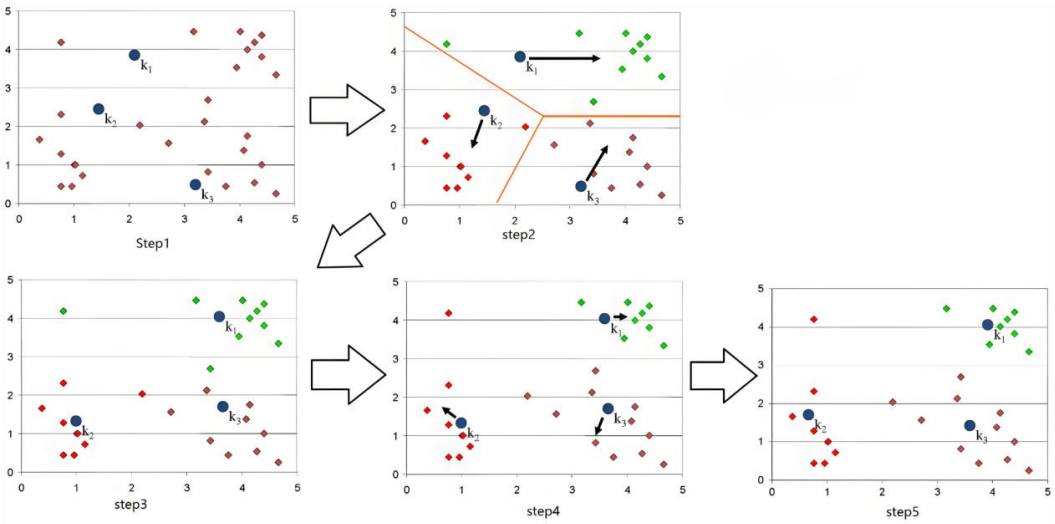

Figure 1: K-means clustering method

3.3.3 Practical Applications: DDoS Defense, Anomaly Detection

Network traffic analysis has wide-ranging applications in practical scenarios, particularly in defending against DDoS attacks and detecting abnormal traffic. DDoS attacks flood target servers with massive amounts of spoofed traffic, causing service disruption. Through traffic analysis, abnormal large-scale traffic patterns can be identified, enabling timely defensive measures such as traffic scrubbing and IP blocking to protect network and server operations. Additionally, traffic analysis can detect abnormal traffic within internal networks, such as unauthorized data transfers, abnormal command executions, and covert malware activities. Real-time monitoring and analysis can uncover and respond to these potential threats early, enhancing overall network security defenses[25].

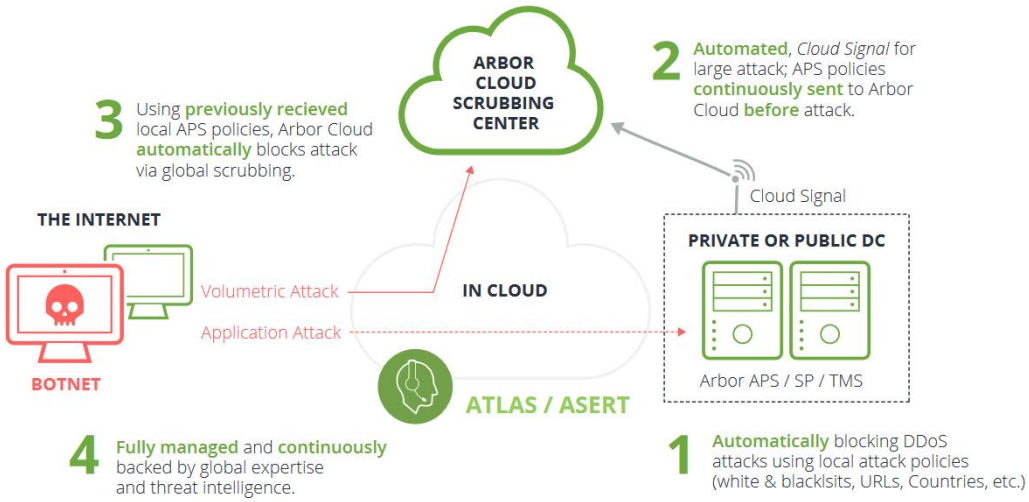

Figure 2: DDoS attack prevention

3.4 Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)

3.4.1 Basic Concepts and Workflow of IDS/IPS

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) are crucial components of cybersecurity for identifying and responding to malicious activities in networks. IDS monitors network traffic and system behavior to identify potential intrusions and issue alerts but does not actively block attacks. IPS, on the other hand, not only detects intrusions but also automatically takes defensive measures, such as blocking malicious traffic or isolating infected devices, when malicious activities are detected. The workflow of IDS/IPS typically includes data collection, feature extraction, pattern matching, decision making, and response. Through real-time monitoring and analysis, IDS/IPS can quickly identify and respond to various network threats, protecting systems and data security[26].

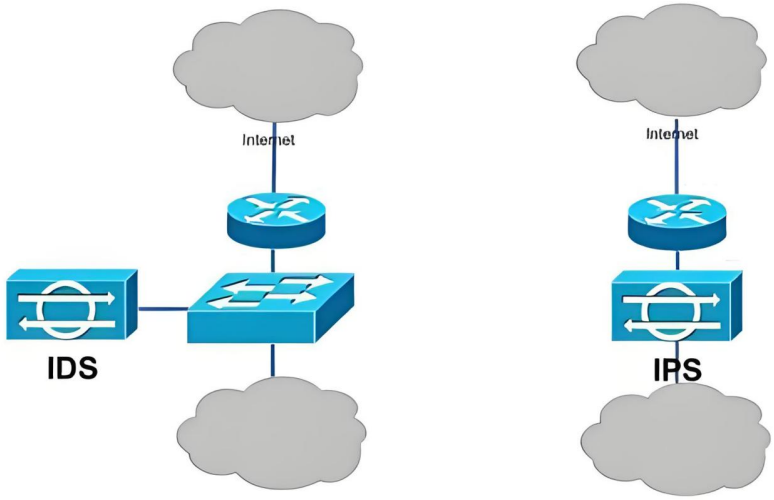

Figure 3: IDS/IPS

3.4.2 Advantages of AI-Based IDS/IPS

AI-based IDS/IPS has significant advantages in threat detection, enhancing accuracy and efficiency. Traditional IDS/IPS systems rely on fixed rules and signature databases, making it difficult to cope with new and complex attack methods. AI-based IDS/IPS, utilizing machine learning and deep learning technologies, can automatically learn and identify complex attack patterns, improving detection capabilities for unknown threats. Additionally, AI algorithms can process vast amounts of data and make rapid decisions and responses in real-time environments, reducing false positives and false negatives. By continuously optimizing and updating models, AI-based IDS/IPS can adapt to changing threat environments, enhancing overall cybersecurity defenses[27].

3.4.3 Common Algorithms: Deep Learning, Ensemble Learning, etc.

In AI-based IDS/IPS, common algorithms include deep learning and ensemble learning. Deep learning algorithms, particularly Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), can automatically extract complex features and identify potential threats in high-dimensional data. Ensemble learning methods, such as Random Forest and Gradient Boosting Trees, combine multiple weak classifiers to improve overall classification accuracy and stability. These algorithms excel in dealing with different types and sizes of threat data and can be selected based on specific needs. By combining the strengths of multiple algorithms, more intelligent and efficient IDS/IPS systems can be built, enhancing cybersecurity defenses[28].

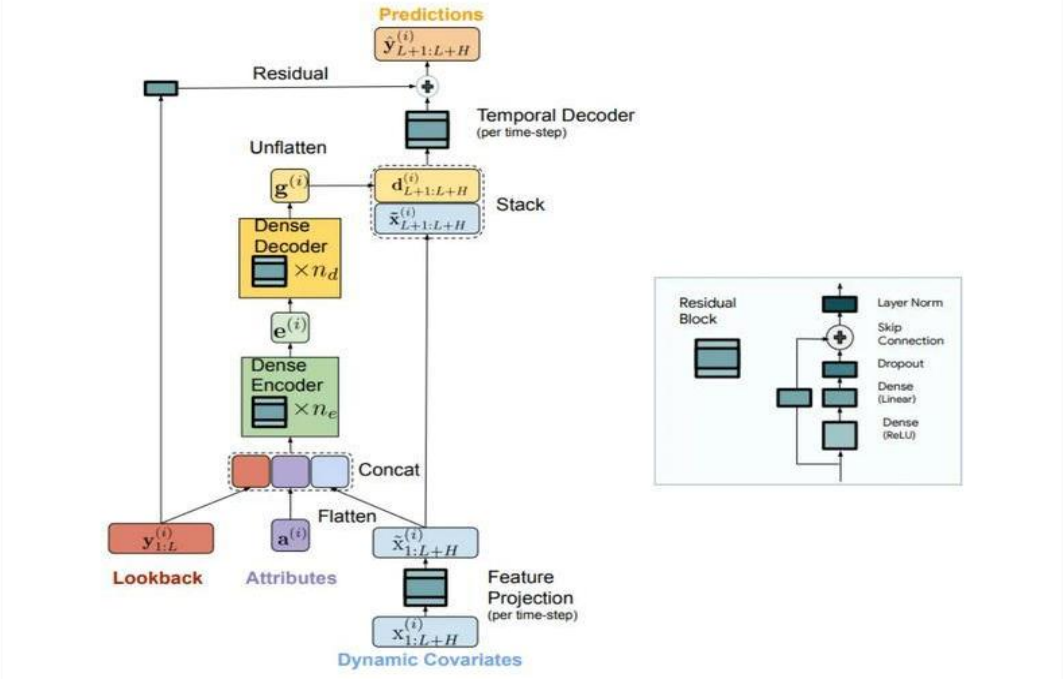

Figure 4: Deep Learning

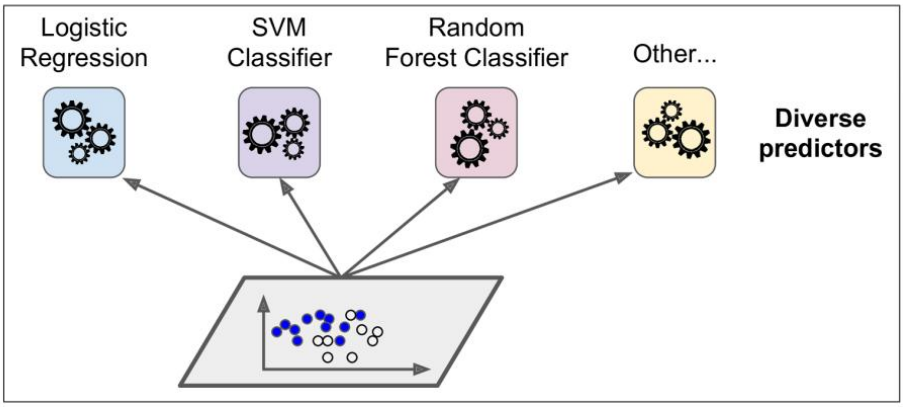

Figure 5: Ensemble Learning

3.5 User Behavior Analysis (UBA)

3.5.1 Definition of User Behavior Analysis

User Behavior Analysis (UBA) is a technique that analyzes user behavior patterns within systems and networks to identify potential insider threats and abnormal behaviors. UBA monitors and analyzes user operation logs, access records, login behaviors, and other information to identify patterns significantly different from normal behaviors, uncovering potential security risks. The core objective of UBA is to enhance the detection capabilities of insider threats through automation and intelligence, preventing data leaks, privilege abuses, and unauthorized accesses. Through continuous monitoring and analysis of user behavior, UBA can build comprehensive cybersecurity situational awareness, detecting and responding to potential threats promptly[29].

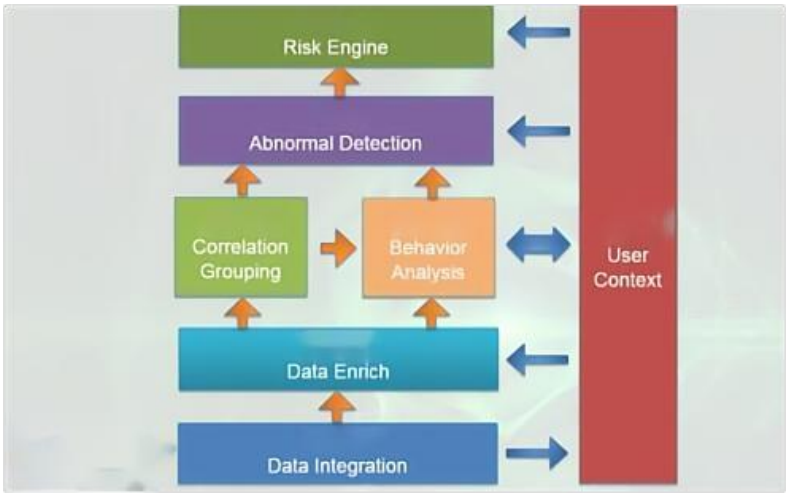

Figure 6: User Behavior Analysis

3.5.2 Common Algorithms: Time Series Analysis, LSTM, RNN, etc.

In user behavior analysis, common machine learning algorithms include time series analysis, Long Short-Term Memory networks (LSTM), and Recurrent Neural Networks (RNN). Time series analysis identifies abnormal time sequences through analyzing user behavior patterns, such as frequent login failures or abnormal timing access patterns. LSTM and RNN are deep learning algorithms, particularly effective for handling sequential data, capturing long-term dependencies and dynamic changes in user behavior. These algorithms excel in processing user behavior data and can be selected based on specific needs. By combining multiple algorithms, the accuracy and efficiency of user behavior analysis can be improved, building a more intelligent insider threat detection system[30].

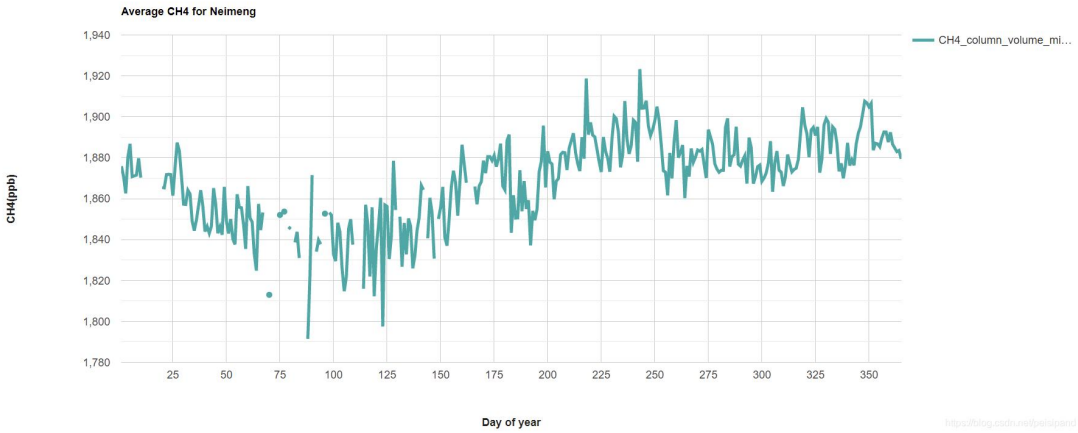

Figure 7: Time Series Analysis

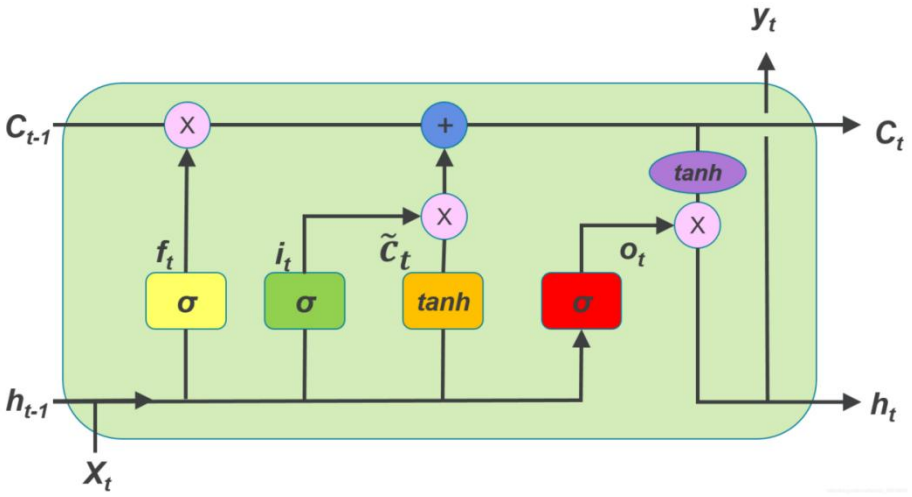

Figure 8: LSTM

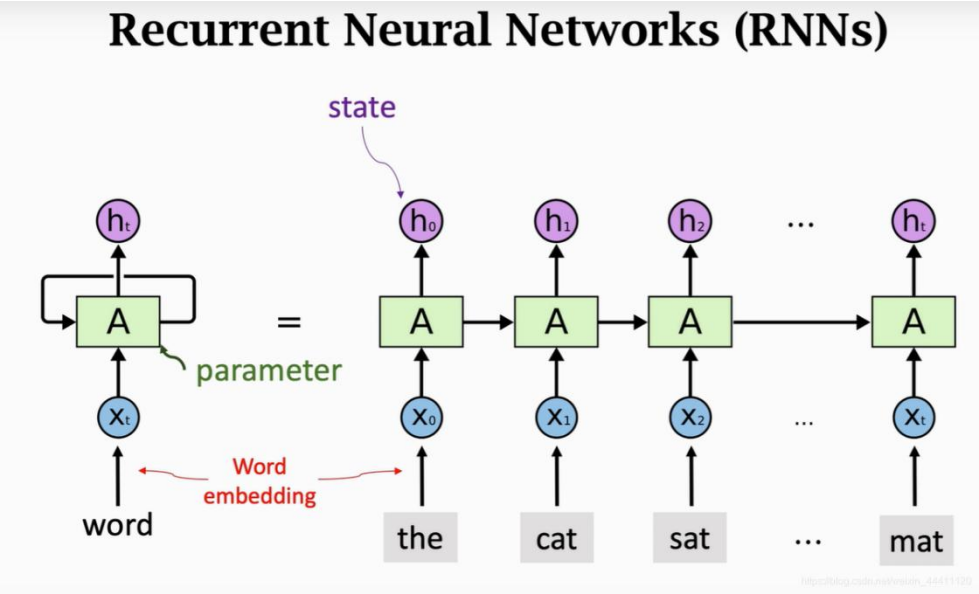

Figure 9: RNN

4. DATA PREPROCESSING AND FEATURE ENGINEERING

4.1 Data Cleaning and Preprocessing

4.1.1 Importance of Data Cleaning

Data cleaning is a critical step in data preprocessing, essential for improving the performance and accuracy of machine learning models. In practical applications, data often contains noise, missing values, duplicates, and outliers, which negatively impact model training and prediction. The goal of data cleaning is to identify and rectify these issues in the data to ensure data quality. High-quality data enhances the generalization capability of models, reducing the risks of overfitting and underfitting. In threat detection, data cleaning is particularly important because security data typically comes from multiple sources with varying formats and quality. Only cleaned data can provide a reliable foundation for subsequent feature engineering and model training.

4.2 Feature Selection and Extraction

4.2.1 Importance of Feature Selection

Feature selection is a critical aspect of feature engineering, crucial for enhancing model performance and interpretability. The goal of feature selection is to select the most representative and informative features from the original set, removing redundant and irrelevant features. By reducing feature dimensionality and computational complexity, feature selection enhances model training speed and prediction accuracy. It also improves model generalization capability, reducing the risk of overfitting. In threat detection, feature selection is particularly important because security data often has high-dimensional features. Effective feature selection can extract the most informative features, improving detection capability and response speed.

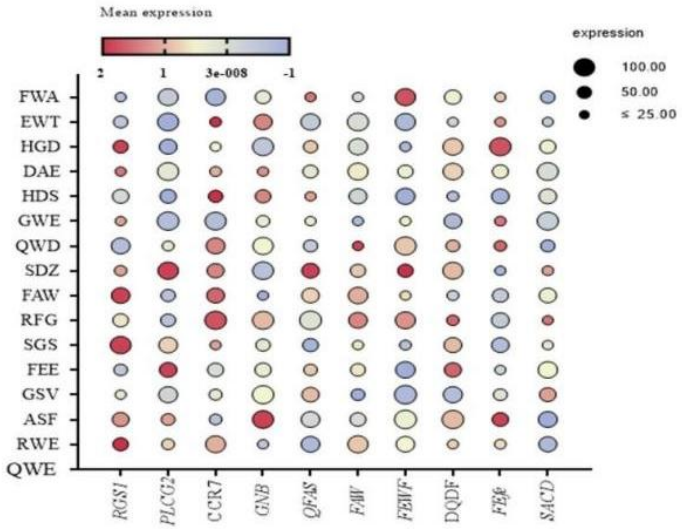

Figure 10: Correlation Analysis

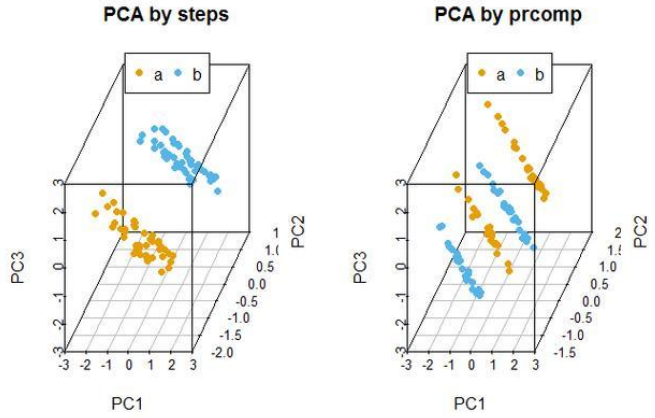

Figure 11: PCA

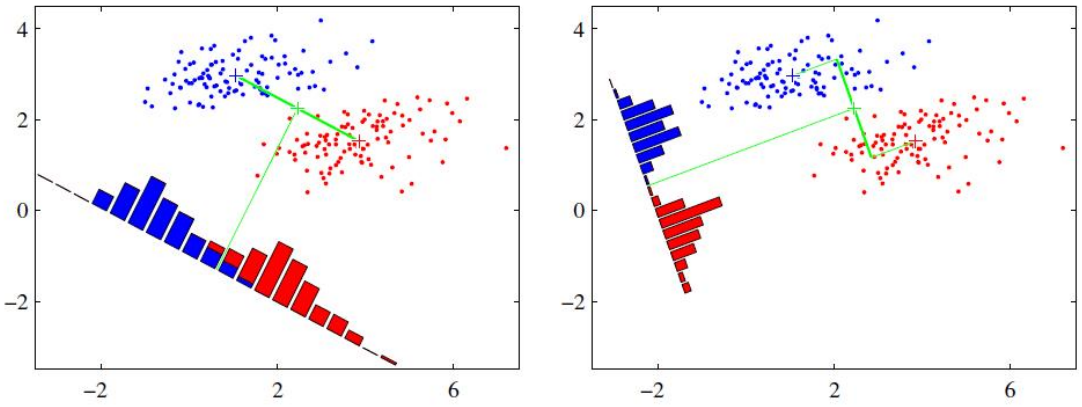

Figure 12: LDA

4.3 Application of Feature Engineering in Threat Detection

4.3.1 Extracting Features from Network Data: Time Features, Protocol Features

Feature engineering plays a crucial role in threat detection by extracting features from network data. Network data typically contains rich time and protocol information, useful for building effective features. Time features include timestamps, time intervals, session duration, and can identify abnormal time patterns and behaviors. Protocol features include protocol types, source/destination ports, flag bits, and can identify abnormal protocol behaviors and attack patterns. For example, by analyzing flag bits and traffic patterns in TCP/IP protocols, potential DDoS attacks and port scanning behaviors can be identified. Extracting these features from network data builds a more comprehensive and effective threat detection model[33].

5. MODEL TRAINING AND EVALUATION

5.1 Model Selection and Hyperparameter Optimization

5.1.1 Model Selection: Machine Learning Models, Deep Learning Models

In threat detection, selecting the appropriate model is crucial for enhancing detection performance. Common models include machine learning models such as Support Vector Machines (SVM), Random Forests, and Gradient Boosting Trees, suitable for structured data, and deep learning models like Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), suitable for large-scale complex data. Model selection considers data type, scale, interpretability, and application requirements. By evaluating the pros and cons of different models, the most suitable model can be chosen to improve threat detection accuracy and efficiency.

5.2 Model Evaluation and Performance Metrics

5.2.1 Common Evaluation Metrics: Accuracy, Recall, F1 Score

Model evaluation is crucial for assessing model performance, using metrics like accuracy, recall, and F1 score. Accuracy measures the proportion of correctly predicted samples to the total samples, evaluating overall prediction capability. Recall measures the proportion of true positive predictions to all actual positive samples, evaluating the model's ability to find positive samples. F1 score is the harmonic mean of accuracy and recall, considering both, suitable for imbalanced class scenarios. By evaluating these metrics, the model's performance can be comprehensively understood, choosing the optimal model for deployment. In threat detection, high recall is particularly important to avoid missing significant security incidents, while high accuracy reduces false positives, enhancing detection reliability.

5.2.2 Confusion Matrix, AUC, ROC Curve

In addition to common metrics, the confusion matrix, AUC, and ROC curve are important tools for model evaluation. The confusion matrix visualizes the correspondence between predicted and actual results, analyzing classification performance and identifying false positives and negatives. AUC (Area Under Curve) measures the area under the ROC curve, evaluating overall classification performance, with higher AUC indicating better performance. The ROC curve plots true positive rate (TPR) and false positive rate (FPR) at different thresholds, showing classification performance and threshold impact, useful for threshold selection and optimization. Comprehensive analysis of these evaluation tools allows a more thorough assessment of model performance, choosing the optimal threshold and model.

6. CHALLENGES IN AI-DRIVEN THREAT DETECTION

6.1 Data Issues

6.1.1 Data Volume, Data Quality, and Labeling Problems

In AI-driven threat detection, data issues are one of the biggest challenges. First, the size of the data volume directly impacts the model's training effectiveness. A large dataset can provide more samples and diversity, which aids in the model's generalization capabilities; however, processing large datasets requires significant

computational resources and time. Second, data quality is another critical issue. High-quality data should be accurate, complete, consistent, and unbiased, but in practice, data often contains noise, missing values, and outliers, all of which can affect the model's performance. Additionally, the accuracy of data labels is crucial. Incorrect labels can lead the model to learn incorrect patterns, thereby affecting detection outcomes. In threat detection, labeling data requires specialized security knowledge and experience, and in practice, there may be issues of inaccurate or missing labels. These issues need to be addressed through data cleaning, preprocessing, and label optimization to improve data quality and usability[36].

6.2 Algorithm Issues

6.2.1 False Positive Rate and False Negative Rate

In AI-driven threat detection, false positive rate and false negative rate are two key performance indicators that directly affect the accuracy and reliability of detection. The false positive rate refers to the proportion of normal behavior mistakenly identified as a threat. A high false positive rate leads to unnecessary alarms and waste of resources. The false negative rate refers to the proportion of real threats that are not detected. A high false negative rate poses serious security risks and losses. To reduce the false positive and false negative rates, suitable models and optimization algorithms need to be chosen, and through feature engineering and hyperparameter optimization, the model's discriminant capabilities and stability can be improved. Additionally, ensemble learning and multi-model fusion methods can be employed to synthesize the predictions of multiple models, thereby reducing errors from individual models. Through comprehensive analysis and optimization, the detection's reliability and practicality can be enhanced while ensuring accuracy and reducing the false positive and false negative rates[37].

7. FUTURE TRENDS

7.1 Smarter Threat Detection

7.1.1 Adaptive Threat Detection Systems

Future threat detection systems will be more intelligent, possessing adaptive capabilities that allow them to automatically adjust detection strategies and model parameters based on changes in the environment and threats. Traditional threat detection systems often rely on fixed rules and models, making them ill-equipped to handle rapidly changing threat situations. Adaptive threat detection systems, on the other hand, can dynamically adjust detection strategies by continuously monitoring and analyzing network traffic and system behavior, thereby improving detection flexibility and accuracy. For example, the system can automatically update models and rules based on current threat intelligence and historical data to optimize detection performance. Furthermore, adaptive systems can enhance their detection capabilities and robustness through self-learning and self-optimization. By comprehensively applying these technologies, future threat detection systems will be better equipped to handle various complex threat scenarios, improving detection efficiency and accuracy and providing stronger security guarantees for network security.

7.2 Cross-Domain Collaboration

7.2.1 Integration of Security and AI Fields

In the future, the integration of the security and AI fields will become even closer, with cross-domain collaboration driving innovation and development in threat detection technology. The application of AI technology in threat detection has already shown significant potential, with machine learning and deep learning technologies enhancing the intelligence level and accuracy of detection. However, the application of AI technology in the security field faces many challenges, such as data quality, algorithm robustness, and adversarial attacks. By strengthening collaboration between the security and AI fields, these challenges can be jointly researched and addressed, driving technological innovation and development. For example, security experts can provide practical threat scenarios and data to help AI researchers develop more practical and effective models and algorithms. At the same time, AI researchers can provide advanced technology and tools to help security experts improve their threat detection and response capabilities. By comprehensively applying these technologies and methods, the continuous innovation and development of threat detection technology can be promoted, providing stronger security guarantees for network security[40].

8. CONCLUSION

8.1 Summary of AI Advantages in Threat Detection

The application of artificial intelligence (AI) technology in threat detection has demonstrated numerous significant advantages. Firstly, AI possesses formidable data processing and analysis capabilities, enabling it to rapidly extract valuable information and patterns from vast datasets. Traditional threat detection methods often rely on rules and feature matching, which struggle to cope with complex and evolving threat scenarios. In contrast, AI technology can automatically learn and identify new threat patterns through machine learning and deep learning algorithms, enhancing detection accuracy and flexibility. Secondly, AI technology has the capability for self-learning and self-optimization. Continuous training and updates can progressively improve the performance and robustness of detection models. This self-learning ability allows AI-driven threat detection systems to dynamically adapt to ever-changing threat environments, promptly identifying and responding to new security threats. Additionally, AI technology can reduce human intervention and enhance detection efficiency and response speed through automation and intelligence, providing more effective and reliable cybersecurity protection. In summary, the application of AI technology in threat detection not only elevates the level of intelligence and accuracy of detection but also enhances overall security defense capabilities, offering robust support in addressing increasingly complex cybersecurity threats.

8.2 Future Research Directions

Despite the significant potential demonstrated by AI in threat detection, numerous challenges remain and are the focus of future research directions. Firstly, data issues continue to be a critical challenge for AI-driven threat detection systems. Future research can concentrate on improving data quality, automating data annotation, and integrating multi-source data. By constructing more comprehensive and high-quality datasets, the training effectiveness and detection performance of models can be enhanced. Secondly, the robustness of algorithms and defense against adversarial attacks are also vital research directions. Researchers can explore more robust models and algorithms, employing techniques such as adversarial training and defensive distillation to bolster model robustness and security, minimizing the impact of adversarial attacks. Furthermore, the real-time performance and response speed of systems need further optimization. Future research can focus on model compression, acceleration technologies, and distributed computing to enhance computational efficiency and resource utilization, achieving more efficient and rapid threat detection. Lastly, cross-domain collaboration and multi-party synergy are emerging as significant trends. By strengthening the integration of security and AI fields and fostering collaboration among governments, businesses, and academia, resource sharing and complementarity can be realized, jointly propelling the innovation and development of threat detection technology. In summary, future research directions will revolve around data quality, algorithmic robustness, system optimization, and cross-domain collaboration. Through continuous technological innovation and practical application, more intelligent, efficient, and reliable threat detection systems will be constructed, providing more robust cybersecurity protection.

REFERENCES

[1] Wang Bingxiang. Research on the Network Security Management Model for Small and Medium-sized Enterprises [J]. Network Security Technology & Application, 2024, (11): 91-95.
[2] Zhang Leiming. Optimization Strategies for Network Security Defense Systems Using Big Data and Artificial Intelligence Technologies [J]. Network Security Technology & Application, 2024, (11): 9-10.
[3] Luo Tianyao, Fang Xiangjie, Li Haolin. Application of Human-Machine Collaborative Network Security Defense Technology in Information Benchmark Schools [J]. Network Security Technology & Application, 2024, (11): 13-15.
[4] Zhu Yao. Research on Network Security Situational Awareness Issues - Based on the Background of Big Data [J]. Network Security Technology & Application, 2024, (11): 20-22.
[5] Zhang Xiaolei. Exploration of College Network Security Practice Based on Situational Awareness [J]. Network Security Technology & Application, 2024, (11): 64-66.
[6] Wang Yan. Reflections on the Construction of Network Security Prevention System in Digital Campuses [J]. Network Security Technology & Application, 2024, (11): 66-68.
[7] Zuo Lijing, Wu Yajun, Zhao Zhuangshi. Discussion on Network Security Protection in District and County-level Government Institutions [J]. Network Security Technology & Application, 2024, (11): 101-103.

[8] Sun Xiaolin, Yuan Yong, Chen Jia. Research on Network Security of Ethnic and Religious Affairs in Universities [J]. Journal of Zunyi Normal University, 2024, 26(05): 141-144.
[9] Xu Tao. Research on the Coordinated Development of Campus Network Security and Information Construction [J]. China Broadband, 2024, 20(10): 103-105.
[10] Sun Baofeng, Zhang Weiyi, Yang Yang, et al. Practice of Network Security Risk Management in Large Hospitals Based on Situational Awareness Platform [J]. Journal of Medical Informatics, 2024, 45(10): 81-85.
[11] Bai Xueyan, A Ri Mu Zha. Cybersecurity Prevention Measures for Chemical Energy Storage Based on Computer Big Data [J]. Energy Storage Science and Technology, 2024, 13(10): 3616-3618. DOI: 10.19799/j.cnki.2095-4239.2024.0820.
[12] Fu Neng. Attack Threats and Countermeasures in Network Security under the Background of Artificial Intelligence [J]. Digital Communication World, 2024, (10): 250-252.
[13] Yan Zheng. Network Security Management and Countermeasures in the Information Construction of Universities [J]. Information System Engineering, 2024, (10): 99-102.
[14] Bai Xue, Zhao Liang. Investigation and Improvement Strategies on the Level of Network Security Literacy among College Students [J]. Journal of Jilin Institute of Chemical Technology, 2024, 41(06): 39-44. DOI: 10.16039/j.cnki.cn22-1249.2024.06.010.
[15] Yang Cui, Zhang En, Liu Xixi, et al. Design of Network Security Course Teaching Model Based on DBL [J]. Computer Education, 2024, (10): 241-245. DOI: 10.16512/j.cnki.jsjjy.2024.10.014.
[16] Chen Jingyao. Research on the Construction of Cybersecurity Protection System in County-level Media Integration Centers under Provincial and Municipal Collaboration [J]. Television Technology, 2024, 48(10): 175-179. DOI: 10.16280/j.videoe.2024.10.047.
[17] Chen Xiaoxin. Strategic Adjustment Paths for Network Security Management in Enterprises under Digital Transformation [J]. Financial Technology Era, 2024, (10): 52-56.
[18] Liang Wenjing, Jiang Jinghui, Tan Weiqi, et al. Construction of an Integrated Network Security Operation System by Guangdong Construction Bank [J]. Financial Technology Era, 2024, (10): 6-11.
[19] The 21st China Cyber Security Annual Conference and the Sub-Forum on Cyber Security Collaborative Governance during the National Cyber Security Publicity Week were Held in Guangzhou [J]. Information Network Security, 2024, 24(10): 1561.
[20] Jiang Wenchao. Exploration of Cybersecurity Information System Construction Based on Artificial Intelligence Technology [J]. Information Recording Materials, 2024, 25(10): 130-132. DOI: 10.16009/j.cnki.cn13-1295/tq.2024.10.058.
[21] SolarWinds Issues Public Sector Cybersecurity Survey Report [J]. Manufacturing Close - Up, 2023,
[22] SolarWinds Brings Out Public Sector Cybersecurity Survey Report [J]. Wireless News, 2023,
[23] World CyberCon Middle East 2023: The Premier Cybersecurity Conference in the Region [J]. M2 Presswire, 2023,
[24] With COVID-19 Behind, New Cybersecurity Spend in Critical Infrastructure to Reach US$236 Billion by 2027 [J]. M2 Presswire, 2023,
[25] Securing Africa's Future: AITEK's Role in the Cybersecurity Industry at GITEX Africa 2023 [J]. M2 Presswire, 2023,
[26] Argonne National Laboratory Collaborating with Exelon to Make EV Charging Stations Cybersecure [J]. Manufacturing Close - Up, 2023,
[27] Juice Jacking Cybersecurity Attack Solution for Consumers & Businesses [J]. M2 Presswire, 2023,
[28] Mark Lynd Releases New Book - Cybersecurity Life Skills for Teens [J]. M2 Presswire, 2023,
[29] He, C., Yu, B., Liu, M., Guo, L., Tian, L., & Huang, J. (2024). Utilizing Large Language Models to Illustrate Constraints for Construction Planning. Buildings, 14(8), 2511. https://doi.org/https://doi.org/10.3390/buildings14082511
[30] Xu, Y., Gao, W., Wang, Y., Shan , X., & Lin, Y.-S. (2024). Enhancing user experience and trust in advanced LLM-based conversational agents. Computing and Artificial Intelligence, 2(2), 1467. https://doi.org/10.59400/cai.v2i2.1467
[31] London entrepreneur joins Saudi Arabian company for ground-breaking cybersecurity project [J]. M2 Presswire, 2023,
[32] Tian, Q., Wang, Z., Cui, X. Improved Unet brain tumor image segmentation based on GSConv module and ECA attention mechanism. arXiv preprint arXiv:2409.13626.
[33] Thales Takes Over Control of ESA's Demonstration Satellite in Pioneering Cybersecurity Drill [J]. Telecomworldwire, 2023,
[34] Xie, Y., Li, Z., Yin, Y., Wei, Z., Xu, G., & Luo, Y. (2024). Advancing Legal Citation Text Classification A Conv1D-Based Approach for Multi-Class Classification. Journal of Theory and Practice of Engineering Science, 4(02), 15-22. https://doi.org/10.53469/jtpes.2024.04(02).03

[35] Xu Y, Shan X, Guo M, Gao W, Lin Y-S. Design and Application of Experience Management Tools from the Perspective of Customer Perceived Value: A Study on the Electric Vehicle Market. World Electric Vehicle Journal. 2024; 15(8):378. https://doi.org/10.3390/wevj15080378
[36] Tier 1 Cyber Security Vendor Selects 2 Silicom Cards [J]. M2 Presswire, 2023,
[37] Skyhigh Report: Majority of IT Professionals Have Experienced a Cybersecurity Breach [J]. Manufacturing Close - Up, 2023,
[38] Jinkui H, Weibin S. Establishment of nonlinear network security situational awareness model based on random forest under the background of big data [J]. Nonlinear Engineering, 2023, 12(1):
[39] The Cyber Report 2023's Best Cybersecurity Firm of the Year - Cyber Sleuth Security [J]. M2 Presswire, 2023,
[40] Skyhigh Report Finds 90% of IT Professionals Have Experienced a Cybersecurity Breach [J]. Wireless News, 2023