Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

AI-Based Cyber Threat Detection in Modern Software Systems

Name: Saif Ali Jogi*

Shaheed Zulfikar Ali Bhutto Institute of Science and Technology (SZABIST), Karachi. Email: livesaifali@gmail.com

Imran Hassan

PhD Scholar, CASE University. FA21MSEE006@caseedupk.onmicrosoft.com

ABSTRACT

The high-paced development of modern software systems, which is described by cloud computing, microservices, the Internet of Things (IoT), and distributed architecture, has greatly increased the area of cyber-attacks, making the traditional signature-based security mechanisms less effective. To overcome these difficulties, artificial intelligence (AI) has been proposed as a groundbreaking strategy to detect cyber threats, which provides predictive, adaptive, and autonomous security features. This review article critically examines AI-based methods of cyber threat detection, which is used in modern software systems. It reviews the literature on machine learning, deep learning, and hybrid AI applications in malware, intrusion attempt, phishing attack, insider threats, and zero-day vulnerability detection. In addition, the review presents information related to data source, feature engineering tactics, and real-time detection models that foster intelligent threat detection in the cloud, IoT, and enterprise settings. The major performance indicators, implementation difficulties, and scalability challenges related to the AI-based security systems are discussed with utmost importance. There is also consideration of ethical concerns such as data privacy, the explainability of the model, and adversarial attacks on the AI systems. This review will additionally illuminate the way forward in developing resilient, explainable, and robust AI-enabled cyber defense systems by integrating current developments and highlights unresolved research gaps that will shape the future of software systems based on next-generation software systems.

Keywords: Artificial Intelligence, Cyber Threat Detection, Software Security, Machine Learning, Deep Learning, Intrusion Detection Systems, Malware Detection,

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Zero-Day Attacks, Cloud Computing Security, Internet of Things (IoT) Security, Adversarial Attacks, Explainable AI.

1. Introduction

The modern software systems are in a completely different state as compared to the past 20 years. Instead, monolithic applications that were locally deployed have been replaced by cloud computing, microservices, distributed architecture, mobile platforms and the proliferating Internet of Things (IoT). The applications today are very much interdependent, data-driven and ever changing. They operate on a variety of networks and platforms. This has increased scalability, flexibility and performance. Nevertheless, it has equally exposed the cyber-attack surface in a vast way, and intricate systems that are interconnected are targets of advanced, automated attacks [1, 2]. Conventionally used security measures like signature-based intrusion detection, rule-based firewalls and off-the-shelf malware scanners were designed to guard the software systems. Reactive tools are based on typically established rules or known signatures, thus failing to notice new malware, polymorphic attacks, advanced persistent attacks, and zero-day weaknesses. Methods of attacks change rapidly, and the volumes and speed of data increase. Traditional tools are unable to offer active, real-time protection [3]. The use of Artificial Intelligence (AI) is changing cybersecurity. AI-based systems rely on machine learning and deep learning to process large volumes of data of different types. They identify multifaceted patterns and detect abnormal behavior which can be an indicator of cyber threats. In contrast to the traditional approaches, AI models gain knowledge with the fresh data, adjust to evolving patterns of attacks, and provide foresight information that enhances software protection. The next generation security solutions have become fundamentally based on AI [4, 5].

The present review discusses AI methods of detecting cyber-threats in contemporary software. It describes the threats of the changing world, explains the data sources and feature engineering, and covers machine learning, deep learning, and hybrid AI. Artificial intelligence security tools in cloud, IoT, and enterprise environments are also discussed in the review. It is intended to inform future studies by outlining challenges and summarizing the existing work to lead to an intelligence,

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

scalable, and robust cyber defense.

In the case of the modern software, the threat environment is diverse, sophisticated, and rapidly changing. Malware is a significant threat such as viruses, worms, trojans, spyware and ransomware. Malicious software in the contemporary world is usually polymorphic or fileless, altering its code or remaining in memory to avoid detection. Ransomware, especially, ciphers valuable information and requires money. Cloud infrastructure, enterprise networks, and vital services are becoming more and more the targets of such attacks, and they use software dependencies or misconfigurations [6, 7]. Network and intrusion attacks are very dangerous. Such attackers are interested in unauthorized access to the network via vulnerabilities in the network, inadequate authentication, or improperly configured services. DDoS attacks flood resources, and the man-in-the-middle attacks destroy confidentiality and integrity. Monitoring large dynamic architectures with significant traffic volumes and variable services is not practical due to the sheer volume of traffic and the inconsistency of services. There is a need to have some smart detection techniques that are able to pick up minor behavioral anomalies [8, 9]. The attacks through phishing and social engineering use human vulnerabilities as opposed to technical vulnerabilities. False emails, websites and messages tempt users to provide credentials or financial information. Threats are evolving at a higher level. Hackers replicate the legitimate communications to the AI-generated content, and the insider threats (both malicious and incompetent) also complicate the issue. Only legitimate access can be used to compromise systems by insiders. They are not easy to detect since it is difficult to discern normal and malicious activity [10-12]. Zero-day vulnerabilities are of critical importance. They exploit undiscovered weaknesses which have no patches or signatures. These exploits may take a long time to be discovered, and they can be extremely harmful. The complexity of the modern ecosystems and its interconnectedness intensifies the effects of the zero-day, which leads to the necessity of behavior-based detection that finds anomalies without any known signatures [13].

2. AI-based Threat detection Data Sources and Feature Engineering

The detection of threats by AI is based on quality and a variety of data. The current

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

systems provide large amounts of data in the form of network traffic, system logs, application logs, and user activity. Packet-level and flow-level information, or source/destination addresses, protocols, traffic volume, captured by network traffic, displays intrusion/DDoS trends. The events, errors, access attempts, and behaviors indicating possible malicious activity are recorded in system and application logs [14, 15]. The data of behavioral and user activity are needed to detect insider threats and compromised accounts. AI can identify abnormal user behavior by executing normal user behavior, alerting of abnormal behavior that shows misuse of credentials or unauthorized access. Raw data obtained through these sources is typically high-dimensional, noisy and redundant. Hence, feature engineering is essential. The feature extraction converts raw data into useful representations, which emphasize statistical attributes, time, protocol-specific attributes [16, 17]. These methods of dimensionality reduction such as Principal Component Analysis (PCA) and autoencoders are useful in simplifying data and preserving important information. Effective feature engineering enhances the accuracy of detection, interpretability of the model, and computational efficiency- important in the real-time detection of threats in a large scale [18, 19].

Table 2.1: ***Common Data Sources and Features for AI-Based Threat Detection***

Data Source	Examples of Features	Targeted Threats
Network Traffic	Packet size, flow duration, protocol type	Intrusions, DDoS
System Logs	Login attempts, error codes, process execution	Malware, insider threats
User Behavior	Access frequency, session duration	Insider threats, phishing

3. Machine Learning Techniques for Cyber Threat Detection

Machine learning (ML) methods are popular to detect cyber threats as it can study patterns based on the data and apply knowledge to new conditions. In cases where there are labeled datasets, supervised algorithms (Support Vector Machines, Random Forests, and k-Nearest Neighbors) are widespread. Such models are suitable in malware classification and intrusion detection, in which historical attacks

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

and their labels are used to train. Nevertheless, supervised models tend to fail where there are unbalanced data and they require regular retraining to remain useful with changing threats [20, 21]. Some of these limitations are alleviated in unsupervised and semi-supervised learning where the normal system behavior is learned without labeled data on attacks. Other algorithms such as clustering algorithms such as k-means and DBSCAN and anomaly detectors such as Isolation Forests are used to identify aberrant data that can indicate malicious intent. Semi-supervised methods are used to integrate small quantities of labeled data, and massive quantities of unlabeled data, providing a workable remedy to the real-world conditions where labeled data is rare [21, 22]. Evaluation MEMLML-based threat detection systems are usually based on the accuracy, precision, recall, F1-score, and detection latency. When it comes to security matters, it is essential to minimize false positives and false negatives since a false classification may lead to alert fatigue or even allow attacks to go undetected. So, ML models have to be fine-tuned and evaluated in the natural environment to guarantee the credible results [23, 24]. Deep learning (DL) has gained interest in cybersecurity due to its capability to automatically acquire hierarchical feature representations by using raw data. Convolutional Neural Networks are suitable in malware detection since they transform binary files into image-like content. LSTM and Recurrent Neural Networks are both useful in sequence modeling and therefore can be used to analyze a network traffic flow and system logs over time [25]. Autoencoders are used to identify abnormalities by training compact normal representations and indicate the differences during reconstruction. As compared to traditional ML methods, DL models can be useful in complex and unseen attacks and can be more effective at addressing them, yet their high computational requirements and inability to be readily understood can impede their use in real-time or resource-constrained environments [26, 27].

4. Intelligent and Hybrid AI Systems

Due to the fact that cyber threats are getting more advanced and dynamic, it is no longer possible to use one method of detection. Hybrid and intelligent AI systems are based on the combination of various computational paradigms to address the weaknesses of single ML or DL models. These systems enhance the accuracy of

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

detection, minimized false positives, and overall generalization to new threats, through the combination of data-informed and domain-knowledge [28, 29]. A hybrid approach combining conventional ML methods and deep learning models is also one of the most frequent. Deep features learned on neural networks are coupled with handcrafted features based on the expertise knowledge (network statistics, protocol indicators, and behavioral metrics). This two-facet methodology retrieves both the low level domain particularity and the high level abstract patterning that would not be exposed in the soles of manual engineering [30]. In intrusion detection, as an example, packet timing statistics may be used in conjunction with deep representations of the raw traffic sequences, which enhance the ability to detect stealthy attacks.

There is the addition of rule-based systems that incorporate AI models, which introduce an additional intelligence layer. Even though rule-based mechanisms are not adaptable, they have a clear contextual awareness and explainability using expert-defined policies. False positives may be significantly decreased when AI-driven warnings are compared with the pre-existing regulations [31]. As an example, an AI model can identify unusual login attempts, a rule layer could be used to determine the activity as scheduled maintenance or trusted locations - thus increasing reliability and interpretability particularly when in a regulated environment.

Reinforcement learning (RL) provides means of dynamical adjustment of cyber defenses. In contrast to the supervised or unsupervised learning, RL allows an agent to acquire optimal security strategies by constantly operating in its environment and receiving feedback in terms of rewards or penalties. Adaptive response to intrusion, automated management of firewalls, and dynamic access control are all applications of RL in the sphere of cybersecurity. These systems are trained to rank threats and optimally use resources and act independently without being explicitly instructed on how to do it [32]. Ensemble learning is also another new line of hybrid AI. Various AI models are used collaboratively to enhance detection strength including decision trees, the neural networks, and anomaly detectors. Ensembles eliminate bias and variance because they average predictions.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

When the pattern of attack is diverse, as in the case of cybersecurity, an ensemble model is better than any single model, as it is more robust to evasion strategies and adversarial strategies [33, 34]. Although they have advantages, hybrid and smart AI systems introduce additional complexity in design, cost of computation, and model management. The complexity of the composition of various elements requires a lot of synchronization to ensure scalability, real-time performance, and continuous flow of data. It is not easy to maintain consistency and trust between different models, especially in scenarios where distributions of data change at any given time. However, these systems are a critical move towards creating resilient, adaptive, and reliable cyber defense solutions that will be capable of addressing the challenges of the modern software systems [35, 36].

5. AI-Based Threat Detection in Emerging Environments

The swift implementation of the new computing paradigms of cloud computing systems, the Internet of Things (IoT), and large-scale enterprise systems have significantly changed the cybersecurity landscape. A large number of stakeholders interact with these environments that produce enormous volumes of heterogeneous, high-velocity data, and run on distributed infrastructures. This is rendering the conventional security methods less effective. Threat detection using AI has thus become the key to guaranteeing security, scalability and resilience in such dynamic and challenging environments [37, 38]. Cloud computing environments are characterized by some special security issues due to their multi-tenant architecture, dynamic allocation of resources and the widespread usage of virtualization and containerization. Cloud systems generate big volumes of telemetry data on a continuous basis - such as network traffic, system logs, and application performance data. This data is used by AI-based security solutions to monitor in real-time, identify anomalies and automatically respond to threats using distributed cloud resources [39]. Deep learning and machine learning models are particularly efficient at identifying the patterns of abnormal resource utilization, unauthenticated access, and side way traffic in cloud systems. Also, AI-based security analytics can handle workload variability and elastic scale, which makes them native to clouds [40]. Nevertheless, the implementation of AI-based threat detection in cloud

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

environments also poses an issue regarding privacy of data, model visibility, and inter-tenant isolation. The challenge of ensuring that AI models do not reveal sensitive information about tenants unintentionally and ensuring that the models can still capture information is a major topic of research. Federated learning and privacy-preserving machine learning are some of the techniques that are being explored to solve these issues as they provide the ability to train models cooperatively without sharing data centrally [41, 42]. Another critical emerging environment that is highly heterogeneous, resource-constrained, and distributed in geography is the Internet of Things. IoT systems comprise sensors, actuators, smart appliances and industrial control systems most of which do not have strong inbuilt security measures. Such devices are frequently used in unprotected locations and are also operating on insecure networks and thus make them easy targets of the cyber-attacks like botnets, spoofing and denial of service attacks. The AI-based threat detection in the IoT setting then needs to strike a balance between computational efficiency and detection accuracy [43, 44]. Smaller machine learning models and edge-based AI have been suggested to overcome the limitations of IoT devices. An AI system can detect threats at the edge or gateway level, which would decrease latency, minimize bandwidth consumption, and respond more quickly to attacks that are local. Autoencoders and more lightweight convolutional networks are deep learning methods that have demonstrated success in identifying the abnormal behavior of devices by learning normal communication patterns. However, IoT devices and protocols are too varied to have generalized detection models, which requires adaptive and context-sensitive AI solutions [45-47]. Threat detection capabilities based on AI are also important to enterprise and distributed software systems. In the modern business world, digital ecosystems are carried out by complex systems incorporating on-premises infrastructure, cloud computing systems, remote workplaces, and third-party applications. This connectivity exposes people to cyber threats, such as insider, credential theft, and advanced persistent threats. AI-based security analytics systems are a collection of various streams of data (network traffic, endpoint logs, identity management systems, user behavior analytics, etc.) that create a coherent, holistic picture of enterprise security [48-50].

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

A comparison between events in multiple data streams shows concealed attack patterns that could be overlooked by isolated security tools. Behavioral analysis using machine-learning detects insider threats and compromised accounts by detecting abnormal user behaviors. Moreover, AI-based automation assists security operations centers with priority of alerts, response time reduction, and alerts fatigue. Nevertheless, to maintain these benefits, AI-based threat detection implementation in an enterprise needs proper governance, explainability, and alignment with the current security processes [51, 52]. In general, AI-threat-detection can be considered a key to securing the emerging computing environments due to scalable, adaptive, and intelligent defense mechanisms. In spite of the fact that issues associated with data quality, privacy, and interpretability remain, the further development of AI technologies makes the cybersecurity solutions more effective and reliable in cloud, IoT, and enterprise systems [37, 53].

6. Challenges and Limitations

Various issues remain a limitation to the deployment of AI-based cyber threat detection systems despite the remarkable progress that has been made in these systems. Data imbalance and labeling is one of the most serious problems. The datasets on cybersecurity are usually extremely skewed, with only a small portion of the data dealt with malicious cases. This is an imbalance that can favor AI models to normal behavior and have a lower detection of rare yet high-impact attacks [54, 55]. Moreover, to acquire correctly labeled security information is time-consuming and costly because it involves professionalism and is constantly updated to comply with the changing trends of attacks [56]. Another significant challenge is scalability, and real-time processing limits, particularly where software systems are of large scale and distributed. To effectively tackle the problem of timely response to threats and counteractions, AI models have to operate with high-velocity data streams at low latencies [57]. Deep learning models are powerful but they can be expensive in terms of computation resources and therefore cannot be deployed easily in resource-constrained settings or in real time settings. Moreover, there is still the issue of keeping performance constant with scale [58]. Another problem that has been persistent in AI-based security systems is false positives and model drift. False

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 1 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

positive rates are high and this may overwhelm security analysts resulting in alert fatigue and lack of confidence in automated detection tools. Model drift arises when the statistical characteristics of the input data are varying with time such that the trained models are no longer effective. On-going retraining and adaptation of the models is thus necessary though it adds further complexity to operations [59, 60].

7. Ethical, Privacy, and Security Concerns

The implementation of AI-based cyber-threat detection creates ethical and privacy concerns. The content of these systems can include sensitive or personally identifiable information and is frequently gathered on a large scale such as the network traffic, system logs, user behavior. The enforcement of data-protection laws and the protection of privacy of the users is a significant issue of concern, particularly on clouds and enterprise physical environments [61]. Xplainable Artificial Intelligence (XAI) is emerging as a necessary tool of credible cybersecurity. A lot of AI and deep-learning models are black boxes, so it is difficult to even comprehend how decisions are made. Inability to explain and investigate incidents will hamper regulatory compliance, user trust, and incident investigation. It is important to fill these shortcomings with the help of interpretable models or post-hoc explanation techniques [62]. Even AI security systems have threats of being attacked by adversarial attacks, where an attacker can modify the input data to avoid being detected or misleading a model. Such attacks as adversarial examples, data poisoning, and model-inversion attacks are posing a risk to the reliability and integrity of AI-driven defenses. To deal with these threats, it is necessary to have tough model design, persistent monitoring, and safe training behaviors [63].

8. Future Directions and Research Gaps

The future research of AI-based cyber-threat detection is aimed at developing self-adapting, autonomous models that can be adapted to deal with the existing and upcoming attacks with minimum human intervention. These systems continuously receive new information, anticipate new attack patterns, and respond in advance to the attacks. Federated learning is an effective strategy that can be used to overcome privacy and collaboration issues. It allows decentralized training of models in many organizations or devices without sharing actual data and thus enhances the accuracy

Online ISSN 3007-3197
Print ISSN 3007-3189

of detection, as well as maintains privacy and regulatory standards. The credible and explainable AI is an important research gap in cybersecurity. The future solutions should be based on high performance in detection and transparency, fairness, and accountability. Effective and interpretable models will be required in order to become widely used in real world security settings.

9. Conclusion

Artificial intelligence (AI) used in cyber threat detection has become an effective and critical means of securing contemporary software systems against more dynamic and sophisticated threats. These systems can provide adaptive, scalable, and intelligent security in cloud, internet of things, and enterprise systems by using machine learning, deep learning, and hybrid AI technologies. Despite such difficulties as data quality, scalability, privacy, and explainability, research is quickly enhancing the efficiency and trustworthiness of AI-based cybersecurity solutions. With more complex and interconnected software systems, the explanation, robust, autonomous and explainable AI defenses will become important in the future of cybersecurity.

10. References

1. Rudrabhatla, C.K.: 'Security design patterns in distributed microservice architecture', arXiv preprint arXiv:2008.03395, 2020
2. Anisetti, M., Ardagna, C., Cremonini, M., Damiani, E., Sessa, J., and Costa, L.: 'Security threat landscape', White Paper Security Threats, 2020
3. Talukder, S.: 'Tools and techniques for malware detection and analysis', arXiv preprint arXiv:2002.06819, 2020
4. Temara, S.: 'Harnessing the power of artificial intelligence to enhance next-generation cybersecurity', 2024
5. Thapaliya, S., and Bokani, A.: 'Leveraging artificial intelligence for enhanced cybersecurity: Insights and innovations', Sadgamaya, 2024, 1, (1), pp. 46-52
6. Kovalchuk, D.: 'Malware development: From early viruses to modern cyber threats', Вісник Черкаського державного технологічного університету. Технічні науки, 2024, 29, (3), pp. 10-20
7. Afreen, A., Aslam, M., and Ahmed, S.: 'Analysis of fileless malware and its evasive behavior', in Editor (Ed.)^(Eds.): 'Book Analysis of fileless malware and

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

its evasive behavior' (IEEE, 2020, edn.), pp. 1-8

8. Ribeiro, A.d.R.L., Santos, R.Y.C., and Nascimento, A.C.A.: 'Anomaly detection technique for intrusion detection in SDN environment using continuous data stream machine learning algorithms', in Editor (Ed.)^(Eds.): 'Book Anomaly detection technique for intrusion detection in SDN environment using continuous data stream machine learning algorithms' (IEEE, 2021, edn.), pp. 1-7
9. Rivera, J.J.D., Khan, T.A., Akbar, W., Afaq, M., and Song, W.-C.: 'An ML Based Anomaly Detection System in real-time data streams', in Editor (Ed.)^(Eds.): 'Book An ML Based Anomaly Detection System in real-time data streams' (IEEE, 2021, edn.), pp. 1329-1334
10. Bhardwaj, Y.: 'The Evolution of Social Engineering: New Threats in the Age of Generative AI', European Journal of Computer Science and Information Technology, 2025, 13, pp. 40-57
11. Schmitt, M., and Flechais, I.: 'Digital deception: Generative artificial intelligence in social engineering and phishing', Artificial Intelligence Review, 2024, 57, (12), pp. 324
12. Kotb, H.M., Gaber, T., AlJanah, S., Zawbaa, H.M., and Alkhathami, M.: 'A novel deep synthesis-based insider intrusion detection (DS-IID) model for malicious insiders and AI-generated threats', Scientific Reports, 2025, 15, (1), pp. 207
13. Zhou, K.-Q.: 'Zero-day vulnerabilities: Unveiling the threat landscape in network security', Mesopotamian Journal of CyberSecurity, 2022, 2022, pp. 57-64
14. Lin, Y.-D., Wang, Z.-Y., Lin, P.-C., Nguyen, V.-L., Hwang, R.-H., and Lai, Y.-C.: 'Multi-datasource machine learning in intrusion detection: Packet flows, system logs and host statistics', Journal of information security and applications, 2022, 68, pp. 103248
15. Xin, J.: 'Application of Multidimensional Data Analysis in Network Intrusion Detection System', International Journal of High Speed Electronics and Systems, 2025, pp. 2540190
16. Singh, M., Mehtre, B., and Sangeetha, S.: 'Insider threat detection based on user

Online ISSN 3007-3197
Print ISSN 3007-3189

behaviour analysis', in Editor (Ed.)^(Eds.): 'Book Insider threat detection based on user behaviour analysis' (Springer, 2020, edn.), pp. 559-574

17. Bin Sarhan, B., and Altwaijry, N.: 'Insider threat detection using machine learning approach', Applied Sciences, 2022, 13, (1), pp. 259
18. Gondhalekar, R., and Chattamvelli, R.: 'A Comprehensive Review of Dimensionality Reduction Techniques for Real time Network Intrusion Detection with Applications in Cybersecurity', Defence Science Journal, 2024, 74, (2), pp. 246-255
19. Verma, J., Sethi, M., Snehi, M., Sharma, I., and Kaushik, K.: 'Optimizing Real-Time Threat Detection with Feature Engineering Strategies for Intelligent NIDS', in Editor (Ed.)^(Eds.): 'Book Optimizing Real-Time Threat Detection with Feature Engineering Strategies for Intelligent NIDS' (IEEE, 2023, edn.), pp. 416-421
20. Xu, W.: 'Advancements in Machine Learning for Network Anomaly Detection: A Comprehensive Investigation'
21. Khanza, A., Yulian, F., Khairunnisa, N., Yusuf, N., and Nuche, A.: 'Evaluating the effectiveness of machine learning in cyber threat detection', Journal of Computer Science and Technology Application, 2024, 1, (2), pp. 172-179
22. Apruzzese, G., Laskov, P., and Tastemirova, A.: 'SoK: The impact of unlabelled data in cyberthreat detection', in Editor (Ed.)^(Eds.): 'Book SoK: The impact of unlabelled data in cyberthreat detection' (IEEE, 2022, edn.), pp. 20-42
23. Salman, T., Ghubaish, A., Unal, D., and Jain, R.: 'Safety score as an evaluation metric for machine learning models of security applications', IEEE Networking Letters, 2020, 2, (4), pp. 207-211
24. Bold, R., Al-Khateeb, H., and Ersotelos, N.: 'Reducing false negatives in ransomware detection: a critical evaluation of machine learning algorithms', Applied Sciences, 2022, 12, (24), pp. 12941
25. Barik, K., Misra, S., Konar, K., Fernandez-Sanz, L., and Koyuncu, M.: 'Cybersecurity deep: approaches, attacks dataset, and comparative study', Applied Artificial Intelligence, 2022, 36, (1), pp. 2055399
26. Hindy, H., Atkinson, R., Tachtatzis, C., Colin, J.-N., Bayne, E., and Bellekens, X.:

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

'Utilising deep learning techniques for effective zero-day attack detection', Electronics, 2020, 9, (10), pp. 1684

27. Sharmila, B., and Nagapadma, R.: 'Quantized autoencoder (QAE) intrusion detection system for anomaly detection in resource-constrained IoT devices using RT-IoT2022 dataset', Cybersecurity, 2023, 6, (1), pp. 41
28. Gupta, A.K., Dixit, N., Kumar, S., and Rawat, P.: 'A Novel Hybrid Approach for Threat Detection in Cyber Security using AI algorithm', in Editor (Ed.)^(Eds.): 'Book A Novel Hybrid Approach for Threat Detection in Cyber Security using AI algorithm' (IEEE, 2024, edn.), pp. 1-6
29. Alserhani, F., and Aljared, A.: 'Evaluating ensemble learning mechanisms for predicting advanced cyber attacks', Applied Sciences, 2023, 13, (24), pp. 13310
30. Gibert, D., Planes, J., Mateu, C., and Le, Q.: 'Fusing feature engineering and deep learning: A case study for malware classification', Expert Systems with Applications, 2022, 207, pp. 117957
31. Palivela, L., Vivekanandan, D., Chinniah, P., Kiranbabu, M., Panneer Dhas, L., and Srivastava, P.: 'Revolutionizing AI decision-making with hybrid rule-based systems: A novel framework for transparent and accurate outcomes', Communications on Applied Nonlinear Analysis, 2024, 31, (8S), pp. 115-127
32. Cadet, E., Etim, E.D., Essien, I.A., Ajayi, J.O., and Erigha, E.D.: 'The role of reinforcement learning in adaptive cyber defense mechanisms', International Journal of Multidisciplinary Research and Growth Evaluation, 2021, 2, (2), pp. 544-559
33. Alqaraleh, S.: 'An Efficient Ensemble Network Anomaly Detection System for Cyber-Attacks', Engineering, Technology & Applied Science Research, 2025, 15, (4), pp. 25549-25554
34. Hussain, L.: 'Fortifying AI Against Cyber Threats Advancing Resilient Systems to Combat Adversarial Attacks', EDRAAK, 2024, 2024, pp. 26-31
35. Moussaoui, J.-E., Kmiti, M., El Gholami, K., and Maleh, Y.: 'A Systematic Review on Hybrid AI Models Integrating Machine Learning and Federated Learning', Journal of Cybersecurity and Privacy, 2025, 5, (3), pp. 41
36. Dari, S.S., Thool, K.U., Deshpande, Y.D., Aush, M.G., Patil, V.D., and Bendale,

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

S.P.: 'Neural Networks and Cyber Resilience: Deep Insights into AI Architectures for Robust Security Framework', Journal of Electrical Systems, 2023, 19, (3)

37. Harshvardhan, C., and Pratikkumar, C.: 'Enhancing cybersecurity in cloud environments using AI-driven threat detection and response', Int. J, 2024, 3, (1), pp. 13-30
38. Uddoh, J., Ajiga, D., Okare, B.P., and Aduloju, T.D.: 'AI-based threat detection systems for cloud infrastructure: Architecture, challenges, and opportunities', Journal of Frontiers in Multidisciplinary Research, 2021, 2, (2), pp. 61-67
39. Ayyadapu, A.K.R.: 'Enhancing Cloud Security with AI-Driven Big Data Analytics', International Neurourology Journal, 2023, 27, (4), pp. 1591-1597
40. Sharma, H.: 'The role of artificial intelligence and machine learning in strengthening cloud security: A comprehensive review and analysis', International Journal of Advanced Research in Computer and Communication Engineering, 2024, 13, (8), pp. 36-44
41. Albshaier, L., Almarri, S., and Albuali, A.: 'Federated learning for cloud and edge security: A systematic review of challenges and AI opportunities', Electronics, 2025, 14, (5), pp. 1019
42. Kodakandla, N.: 'Federated learning in cloud environments: Enhancing data privacy and AI model training across distributed systems', International Journal of Science and Research Archive, 2022, 5, (2), pp. 347-356
43. Zaman, S., Alhazmi, K., Aseeri, M.A., Ahmed, M.R., Khan, R.T., Kaiser, M.S., and Mahmud, M.: 'Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey', Ieee Access, 2021, 9, pp. 94668-94690
44. Sunkara, G.: 'AI-driven cybersecurity: Advancing intelligent threat detection and adaptive network security in the era of sophisticated cyber attacks', Well Testing Journal, 2022, 31, (1), pp. 185-198
45. Obuse, E., Ayanbode, N., Cadet, E., Etim, E.D., and Essien, I.A.: 'Edge AI solutions for real-time IoT device threat monitoring', International Journal of Scientific Research in Computer Science, Engineering and Information

Online ISSN 3007-3197
Print ISSN 3007-3189

Technology, 2024, 10, (3), pp. 996-1030

46. Catillo, M., Pecchia, A., and Villano, U.: 'A deep learning method for lightweight and cross-device IoT botnet detection', Applied Sciences, 2023, 13, (2), pp. 837
47. Figueroa, N., Priya, V., Shanmugam, S., Kumar, K., Sengan, S., and Bolivar, A.: 'Adaptive approach to anomaly detection in Internet of Things using autoencoders and dynamic thresholds', Journal of Machine and Computing, 2024, 4, (1), pp. 1-10
48. Kwentoa, I.K.: 'AI-Driven Threat Intelligence for Enterprise Cybersecurity', Journal of Next-Generation Research 5.0, 2025
49. Khan, P., Islam, M.Z., and Hossain, S.: 'AI-Powered Cybersecurity: Revolutionizing Business Threat Detection and Response'
50. Sivakumar, J., Salman, N.R., Salman, F.R., Salimova, H.R., and Ghimire, E.: 'AI-driven cyber threat detection: enhancing security through intelligent engineering systems', Journal of Information Systems Engineering and Management, 2025, 10, (19), pp. 790-798
51. Ravikumar, N.: 'AI-Supported Cybersecurity Monitoring in Enterprise Environments: Enhancing Threat Detection and Response', Emerging Frontiers Library for The American Journal of Engineering and Technology, 2025, 7, (11), pp. 55-64
52. ABEL, U., EMMANUEL, C., and PASCAL, U.O.: 'Applying artificial intelligence in Cybersecurity to enhance threat detection, response, and risk management', COMPUTER SCIENCE, 2024, 5, (10), pp. 2511-2538
53. Joshua, E., and Mylavarapu, P.: 'AI-driven threat detection: Enhancing cybersecurity automation for scalable security operations', Int. J. Sci. Res. Arch, 2025, 14, (3), pp. 681-704
54. Pawlicki, M., Choraś, M., Kozik, R., and Hołubowicz, W.: 'On the impact of network data balancing in cybersecurity applications', in Editor (Ed.)^(Eds.): 'Book On the impact of network data balancing in cybersecurity applications' (Springer, 2020, edn.), pp. 196-210
55. Bagui, S., and Li, K.: 'Resampling imbalanced data for network intrusion

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

detection datasets', Journal of Big Data, 2021, 8, (1), pp. 6

56. Guerra, J.L., Catania, C., and Veas, E.: 'Datasets are not enough: Challenges in labeling network traffic', Computers & Security, 2022, 120, pp. 102810
57. Zhang, H., Jia, X., Chen, C., Bachani, S., Goel, J., Tarun, M., Mahmood, H.-A.R., Abdullah, B.A., Talib, R.M., and Nasir, N.A.: 'Deep learning-based real-time data quality assessment and anomaly detection for large-scale distributed data streams', International Journal of Medical and All Body Health Research, 2025, 6, (1), pp. 01-11
58. Shuvo, M.M.H., Islam, S.K., Cheng, J., and Morshed, B.I.: 'Efficient acceleration of deep learning inference on resource-constrained edge devices: A review', Proceedings of the IEEE, 2022, 111, (1), pp. 42-91
59. Preuveneers, D., Llamas, J.M., Bulut, I., Rúa, E.A., Verfaillie, P., Demortier, V., Surinx, D., and Joosen, W.: 'On the use of AutoML for combating alert fatigue in security operations centers', in Editor (Ed.)^(Eds.): 'Book On the use of AutoML for combating alert fatigue in security operations centers' (Springer, 2023, edn.), pp. 609-627
60. Ying, J., Zhu, T., Zheng, A., Chen, T., Lv, M., and Chen, Y.: 'METANOIA: A Lifelong Intrusion Detection and Investigation System for Mitigating Concept Drift', arXiv preprint arXiv:2501.00438, 2024
61. SRIDEVI, K., MUHAMMAD, A.F., and MUHAMMAD, A.: 'Privacy-preserving AI for cybersecurity: Balancing threat intelligence collection with user data protection', INTERNATIONAL JOURNAL, 2021, 2, (2), pp. 280-292
62. Agarwal, G.: 'Explainable AI (XAI) for Cyber Defense: Enhancing Transparency and Trust in AI-Driven Security Solutions', International Journal of Advanced Research in Science, Communication and Technology, 2025, 5, (1), pp. 132-138
63. Rahman, M.M., Arshi, A.S., Hasan, M.M., Mishu, S.F., Shahriar, H., and Wu, F.: 'Security risk and attacks in AI: A survey of security and privacy', in Editor (Ed.)^(Eds.): 'Book Security risk and attacks in AI: A survey of security and privacy' (IEEE, 2023, edn.), pp. 1834-1839