 ISSN: 3107-6513

AI-Based Behavioral Analytics Detection System for Enhancing Incident Response and Incident Handling of Labeled and Unlabeled Cyber Attacks

[1]Sharma Aayush Sharad, [2]Mullaji Zoya Rafique, [3]Jayesh Shinde
[1,2,3]M.S.(Cybersecurity),[1,2] Student, [3]Professor
Department of Information Technology, University of Mumbai Vidyanagari, Kalina, Santacruz, Mumbai, Maharashtra, India
[1]Sharmaaayushsharad333@gmail.com,[2] zoyamullaji7@gmail.com,[3] shinde.jayesh2005@gmail.com

Abstract - The rapidly evolving cyber threat landscape has reduced the effectiveness of traditional incident response and incident handling approaches. Organizations today must protect their systems from both labeled attacks, which follow known and documented patterns, and unlabeled attacks, such as zero-day exploits and previously unseen threats. Security solutions that rely on static signatures and predefined rules are increasingly inadequate in this environment. These systems often fail to identify new or emerging threats and tend to generate a high volume of false alerts. As a result, security teams experience delayed threat detection, longer attacker dwell times, and increased operational risk. This paper examines how AI-based behavioral analytics detection systems can strengthen incident response and incident handling processes for both labeled and unlabeled cyber attacks. It reviews the incident response lifecycle and analyzes how behavioral analytics improves detection accuracy, alert prioritization, and overall response effectiveness. Based on existing research, the study evaluates the performance of supervised, unsupervised, semi-supervised, and deep learning techniques applied to cybersecurity detection. Particular focus is placed on anomaly detection methods that learn normal system behavior and identify deviations that may indicate malicious activity. The paper also discusses how AI-driven behavioral analytics supports greater automation, reduces response delays, and enhances decision-making within Security Operations Centers. Although challenges related to model interpretability, data quality, and deployment complexity remain, the integration of adaptive and intelligence-driven detection systems is a critical step toward developing more resilient and scalable cyber defense mechanisms.

Key Words: Incident Response, Incident Handling, Labeled Attacks, Unlabeled Attacks, Cybersecurity, Threat Detection, Behavioral Analytics, Anomaly Detection

I. INTRODUCTION

The cybersecurity landscape has changed significantly over the past decade due to the rapid advancement of attack techniques, the growing sophistication of threat actors, and the widespread digitalization of organizational systems. Traditional perimeter-based defenses and static detection methods are no longer adequate for protecting modern infrastructures against highly dynamic and adaptive cyber threats. The emergence of zero-day exploits, polymorphic malware, ransomware campaigns, and long-term advanced persistent threats has highlighted the fundamental weaknesses of conventional security approaches [4][19]. Signature-based intrusion detection systems (IDS) and rule-based security tools depend heavily on predefined attack patterns and known indicators of compromise. Although these methods are effective for detecting previously identified threats, they are inherently limited when it comes to identifying novel attacks that lack historical signatures. Attackers increasingly take advantage of this gap by creating new malware variants, obfuscating malicious payloads, and abusing legitimate system behavior to bypass detection mechanisms. As a result, many modern intrusions go unnoticed for extended periods, allowing adversaries to maintain persistence and amplify their impact over time [11][24]. AI-based behavioral analytics introduces a fundamental shift in cybersecurity detection strategies. Instead of relying solely on known attack signatures, behavioral analytics systems establish baselines of normal system, network, and user behavior and detect deviations that may signal malicious activity. By applying machine learning and deep learning techniques, these systems are capable of processing large volumes of diverse data, identifying subtle behavioral anomalies, and adapting to continuously changing environments. This approach enables the detection of both labeled attacks, where historical data and labels are available, and unlabeled attacks, including zero-day and previously unseen threats [6][9][13]. Beyond enhancing detection capabilities, AI-driven behavioral analytics also strengthens incident response processes by enabling faster alert generation, better alert prioritization, and higher levels of automation. Automated correlation, risk assessment, and response orchestration help reduce the workload on security analysts and significantly decrease the time between detection and mitigation. As a result, organizations are better positioned to limit the impact of attacks and improve their overall security posture [1][3][14].

II. LITERATURE REVIEW

2.1 Evolution of the Cyber Threat Landscape

The contemporary cyber threat environment is characterized by increasing complexity, scale, and persistence. Advanced persistent threats, zero-day exploits, ransomware, supply chain attacks, and insider threats have become prevalent across industries (Behl and Behl [1]; Conti et al. [14]). These threats are often multi-stage, stealthy, and designed to evade traditional detection mechanisms. Attackers increasingly employ polymorphic and metamorphic techniques, dynamically altering malware behavior to avoid signature-based identification (Sommer and Paxson [19]; Bilge and Dumitras [24]). Zero-day attacks pose a particularly serious challenge, as they exploit unknown vulnerabilities for which no patches or signatures exist (Bilge and Dumitras [24]). The time gap between vulnerability discovery and remediation creates a critical exposure window during which attackers can operate undetected. Insider threats further complicate detection efforts, as malicious activity may closely resemble legitimate behavior and evade rule-based monitoring systems (Greitzer and Frincke [23]). The adoption of cloud computing, hybrid infrastructures, and Internet of Things (IoT) technologies has significantly expanded the attack surface. Distributed architectures generate massive volumes of telemetry across diverse platforms, making centralized monitoring and correlation increasingly difficult. Industrial control systems and smart factory environments introduce additional complexity due to their real-time constraints and safety-critical operations (Mitchell and Chen [27]; Humayed et al. [29]). These developments necessitate detection systems capable of real-time analysis, cross-domain correlation, and continuous adaptation (Behl and Behl [1]; Killcrece et al. [14]; Patcha and Park [15]).

2.2 Limitations of Traditional Detection Systems

Traditional cybersecurity defenses, including signature-based intrusion detection systems, firewalls, and static security policies, exhibit several well-documented limitations. First, they are inherently incapable of detecting unknown or novel attacks, as detection relies on pre-existing knowledge. Second, rule-based systems frequently generate high volumes of false positives, overwhelming analysts and contributing to alert fatigue (Axelsson [5]; SANS Institute [18]). Third static detection rules lack adaptability and cannot evolve in response to changing network behavior or attack strategies. Fourth, traditional systems focus on isolated events rather than analyzing behavioral patterns over time, limiting their ability to detect slow-moving or multi-stage attacks. Finally, heavy reliance on manual investigation and response increases mean time to detect (MTTD) and mean time to respond (MTTR), allowing attackers to persist within compromised environments (Bilge et al. [4]; Killcrece et al. [12]). These limitations have been consistently highlighted in the literature and serve as a primary motivation for adopting learning-based detection approaches (Sommer and Paxson [19]).

2.3 AI and Behavioral Analytics Paradigm

AI-based behavioral analytics introduces a fundamentally different detection philosophy by focusing on behavior rather than signatures. Behavioral profiling involves constructing models of normal activity for users, devices, applications, and networks. Anomalies are identified when observed behavior deviates significantly from established baselines (Bishop [10]; Chandola et al. [13]). Machine learning and deep learning techniques enable scalable implementation of behavioral analytics by automating feature extraction, pattern recognition, and decision-making. Temporal analysis allows systems to detect long-term or multi-stage attacks, while contextual awareness improves accuracy by incorporating environmental information and threat intelligence (Kim et al. [9]; Hochreiter and Schmidhuber [11]). Adaptive learning mechanisms further enable continuous model updates to reflect evolving behavior and emerging threats (Bhuyan et al. [6]; Sommer and Paxson [19]).

III. METHODOLOGY

3.1 Supervised Learning Techniques

Supervised learning techniques are commonly applied to the detection of labeled cyber-attacks, where historical datasets and ground-truth labels are available. Benchmark datasets such as CICIDS-2017/2018, UNSW-NB15, and NSL-KDD provide labeled instances of benign and malicious network traffic and are widely used to evaluate detection performance [6][9]. Feature engineering is a critical component of supervised learning, as it involves extracting meaningful behavioral features such as traffic volume, session duration, protocol usage, packet timing, and resource access patterns. Algorithms like Decision Trees offer transparency and interpretability, allowing analysts to understand how classification decisions are made. Random Forest models enhance robustness through ensemble learning, while gradient boosting methods such as XGBoost are capable of capturing complex non-linear relationships, leading to improved detection accuracy [12][18]. The outputs generated by supervised learning models are integrated into incident response workflows to support alert prioritization and automated mitigation. Confidence scores and contextual insights derived from these models assist analysts in making informed decisions and help reduce response times [3].

3.2 Unsupervised Learning for Anomaly Detection

Unsupervised learning plays a crucial role in detecting unlabeled and zero-day attacks, particularly in scenarios where labeled training data is unavailable. These approaches focus on learning patterns of normal system behavior and identifying deviations that may indicate malicious activity [11][23]. Isolation Forest algorithms detect anomalies by isolating rare and distinct data points, making them suitable for large-scale cybersecurity datasets. Autoencoder-based methods learn compact representations of normal behavior

and identify anomalies based on reconstruction error. One-Class Support Vector Machine (SVM) models establish boundaries around normal activity and detect deviations within high-dimensional feature spaces [13][24]. Anomaly scores produced by these models are correlated and normalized to reduce false positives, with high-risk anomalies forwarded to incident response systems for further investigation and mitigation [26].

3.3 Semi-Supervised and Hybrid Approaches Semi-supervised learning techniques combine limited labeled data with large volumes of unlabeled data to enhance detection performance. Methods such as pseudo-labeling and clustering support label propagation and facilitate the detection of evolving threats that partially resemble known attack patterns [25][30]. Hybrid detection architectures integrate supervised, unsupervised, and semi-supervised models within a unified pipeline. Ensemble methods and weighted scoring mechanisms improve robustness, resistance to evasion, and overall scalability, while enabling greater adaptability to changing threat environments [28].

3.4 Deep Learning Architectures
Deep learning models are well suited for capturing complex, non-linear, and temporal attack behaviors. Long Short-Term Memory (LSTM) networks model sequential dependencies in logs and network traffic, supporting the detection of persistent threats. Convolutional Neural Networks (CNNs) extract spatial features from structured data, while CNN–LSTM hybrid architectures enable the identification of multi-stage attacks. Autoencoders and variational autoencoders further support robust anomaly detection, even in the presence of noisy data [9][11][19].

3.5 Emerging Techniques: Federated Learning and Reinforcement Learning
Federated learning enables collaborative model training across distributed environments without requiring the sharing of raw data, thereby supporting privacy preservation and regulatory compliance. Reinforcement learning approaches optimize response strategies through adaptive feedback mechanisms, allowing for dynamic and automated incident response processes [1][3][22].

IV. FINDINGS & ANALYSIS

4.1 Performance Metrics Across Systems
An analysis of existing studies indicates that AI-based behavioral analytics systems consistently outperform traditional signature-based detection approaches [1], [3], [5]. Across diverse attack scenarios, these systems achieve high levels of accuracy, precision, recall, and F1-scores [6], [8]. At the same time, they demonstrate a significant reduction in both false positives and false negatives, underscoring the effectiveness of learning-based techniques in dynamic and evolving threat environments [9], [11]. AI-driven automated incident response frameworks frequently report mean F1-scores exceeding 90%, along with measurable reductions in detection errors and response delays [12], [14]. Behavioral analytics–based UEBA systems outperform rule-based SIEM platforms by lowering false-positive rates and shortening incident triage times [15], [17]. Deep learning–based web security solutions further demonstrate strong scalability and robustness, achieving near-perfect F1-scores on large real-world datasets [18], [19]. Similarly, log-based anomaly detection frameworks maintain high detection accuracy while improving computational efficiency [20]. Recent advancements also show that large language models can achieve high intrusion detection accuracy even when limited labeled data is available through in-context learning techniques [21], [22]. These models perform effectively in areas such as cloud security, malware detection, and container misconfiguration analysis [23]. Federated and adaptive AI frameworks further reduce detection latency while preserving high accuracy, enabling near real-time security operations [24], [25]. Evaluations conducted using standard benchmark datasets, including CICIDS-2017, UNSW-NB15, and CSE-CIC-IDS2018, confirm consistent performance improvements across systems [26], [27]. Overall, the evidence clearly demonstrates that AI-based behavioral analytics provides a substantial advantage over traditional detection methods, particularly in identifying emerging threats and supporting real-time response capabilities [28]–[30].

4.2 Zero-Day and Unlabeled Attack Detection One of the most significant strengths of AI-based behavioral analytics lies in its ability to detect zero-day and previously unseen attacks [2], [6]. Unsupervised and semi-supervised learning techniques are particularly effective in this context, as they model normal behavior and identify deviations that may indicate malicious activity [7], [9]. Encoder–decoder architectures and recurrent neural networks have proven successful in detecting real-world zero-day web attacks that bypass conventional security controls [10], [13]. Open-set recognition techniques further enhance detection capabilities by enabling systems to identify unknown attack classes and dynamically update detection models, thereby overcoming the limitations of closed-set classifiers [14], [16]. Deep learning–based behavioral anomaly detection strengthens zero-day detection by assigning risk scores based on deviations from learned behavioral baselines [18], [20]. Semi-supervised learning approaches improve detection performance for rare and emerging attack types by effectively leveraging unlabeled data and reducing dependence on large labeled datasets [21], [23]. Recent studies also demonstrate that large language models are capable of identifying previously unseen IoT attacks, highlighting their potential applicability in zero-day detection scenarios [24], [25]. Collectively, these findings strongly support the effectiveness of AI-driven behavioral analytics in identifying zero-day and unlabeled attacks through adaptive, data-driven learning mechanisms [26]–[30].

4.3 Incident Response Automation and Latency Reduction
Beyond threat detection, AI-driven automation plays a critical role in enhancing incident response and incident handling processes [3], [12]. Federated and agent-based AI frameworks enable autonomous threat hunting, cross-environment correlation, and real-time mitigation, achieving high levels of automated containment for advanced threats such as ransomware [15], [18]. Advanced decision-making systems that integrate game-theoretic models with deep

reinforcement learning optimize response strategies in adversarial environments [19], [22]. These approaches demonstrate strong performance in automated response planning, achieving near-optimal outcomes in simulated attack and defense scenarios [23]. Collaborative intrusion prevention architectures further reduce response latency by tightly coupling detection and mitigation workflows [24], [26]. Behavioral analytics–based UEBA frameworks significantly reduce incident triage time, allowing security teams to respond more quickly while simultaneously reducing analyst workload [27], [28]. Many systems achieve real-time processing with millisecond-level end-to-end latency, resulting in substantial reductions in both detection and response times [29], [30]. Adaptive defense mechanisms further enhance system resilience by continuously adjusting security controls in response to evolving threat intelligence [25], [28]. These results highlight the importance of AI-driven automation in minimizing the time between detection and mitigation and in reducing overall attack impact.

4.4 Application Domain Analysis

AI-based behavioral analytics systems demonstrate high versatility and applicability across a wide range of cybersecurity domains [1], [5]. In multi-cloud and hybrid environments, federated AI frameworks address challenges related to fragmented telemetry, inconsistent security policies, and cross-platform threat correlation [24], [26]. Network intrusion detection remains a key application area, with consistently high detection accuracy reported across standard benchmark datasets [27], [28]. In web application security, behavioral analytics systems effectively detect zero-day attacks that are often missed by traditional web application firewalls [6], [10]. Endpoint protection platforms leverage AI-driven malware behavior analysis to identify zero-day ransomware and complex multi-stage intrusions [11], [14]. In industrial control systems and smart manufacturing environments, deep learning–based collaborative intrusion prevention systems address the unique security requirements of Industrial IoT networks [16], [18]. IoT security benefits from AI-based anomaly detection and cyber twin technologies [20], [21], while cloud security platforms demonstrate strong performance in malware detection, traffic anomaly classification, and configuration analysis [22], [23]. Insider threat detection is enhanced through UEBA frameworks and unsupervised deep learning models [25], [27]. Encrypted traffic analysis further highlights the effectiveness of semi-supervised and resilient anomaly detection techniques [28], [29]. Overall, the breadth of successful applications underscores the adaptability, scalability, and practical value of AI-based behavioral analytics within modern cybersecurity environments [30].

V. DISCUSSION

5.1 Strengths and Advantages

AI-based behavioral analytics provides several clear advantages over traditional cybersecurity approaches [1], [4]. One of its most significant strengths is the ability to detect novel and zero-day attacks [6], [9]. By learning baseline patterns of normal behavior and identifying deviations, unsupervised and semi-supervised models can uncover previously unseen threats that signature-based detection systems are unable to identify [10], [13]. These approaches also demonstrate high detection accuracy while producing substantially fewer false positives [15], [17]. Another important advantage is the ability to support real-time analysis with low latency [18], [19]. Advanced system architectures are capable of processing events and generating alerts within milliseconds, enabling organizations to respond rapidly before attacks escalate or cause significant damage [20], [22]. The automation of incident response processes further improves effectiveness by reducing the time between detection and mitigation [23], [24]. In addition, adaptability and continuous learning capabilities help ensure long-term effectiveness in dynamic and evolving threat environments [25], [26].

5.2 Challenges and Limitations

Despite these advantages, several challenges continue to affect the effectiveness and practical adoption of AI-based behavioral analytics systems [3], [7]. The limited availability of high-quality labeled datasets, along with severe class imbalance, complicates both model training and performance evaluation [8], [11]. Adversarial threats, including data poisoning and evasion attacks, also present increasing risks to detection reliability [12], [14]. Model interpretability remains a major concern, as many deep learning techniques function as black-box systems, making decision processes difficult to explain [16], [18]. High computational requirements can restrict deployment in resource-constrained environments [19], [20]. Additionally, encrypted traffic and concept drift pose ongoing challenges to maintaining long-term detection accuracy and system relevance [21], [23].

5.3 Practical Deployment Considerations

Successful deployment of AI-based behavioral analytics systems requires seamless integration with existing SIEM and SOAR platforms [24], [25]. Accurate baseline modeling, adaptive thresholding, and human-in-the-loop workflows remain critical to maintaining detection reliability and operational trust [26], [27]. Privacy and regulatory requirements can be addressed through federated and privacy-preserving learning approaches [28], [29]. Finally, continuous monitoring, periodic retraining, and careful scalability planning are essential to ensure sustained performance and long-term operational effectiveness [30].

VI. FUTURE RECOMMENDATIONS

Looking ahead, several research and development directions can further strengthen AI-based behavioral analytics and incident response systems [1], [5]. Improving explainability and interpretability remains a top priority [10], [19]. Cybersecurity-specific explainability techniques, including neuro-symbolic approaches that integrate machine learning with logical reasoning, can enhance transparency, build trust, and support regulatory compliance [15], [19]. Enhancing robustness against adversarial threats is equally critical [28]. Ongoing research into poisoning-resistant models, adversarial training strategies, and standardized robustness evaluation frameworks will help protect detection systems from increasingly sophisticated attacks [17], [28]. The availability of realistic zero-day datasets continues to be a

major challenge [4], [24]. Approaches such as synthetic data generation, adversarial simulations, and collaborative data-sharing initiatives offer promising solutions to current data limitations [6], [18]. Expanding the use of federated and privacy-preserving learning techniques will enable cross-organizational collaboration while maintaining strong privacy guarantees [1], [24]. Methods such as differential privacy can further strengthen these frameworks [25], [28]. The integration of large language models presents new opportunities for contextual threat intelligence, natural language–driven threat hunting, and automated documentation [7], [22]. At the same time, addressing risks specific to large language models, including prompt injection, remains essential to ensure secure deployment [7], [22]. Multi-modal behavioral analytics, which combines network traffic, system logs, user behavior, endpoint telemetry, and threat intelligence, can provide richer and more comprehensive situational awareness [16], [19]. Graph-based modeling approaches that capture relationships among entities show particular promise in this area [21], [29]. Further advances in automated response orchestration, supported by reinforcement learning and adaptive playbook generation, can reduce response times, provided that appropriate safeguards are implemented to ensure safe and reversible actions [3], [14], [22].

Supporting continuous learning and adaptation through online learning frameworks will improve long-term system effectiveness while reducing retraining costs [9], [26]. Achieving an appropriate balance between model stability and adaptability remains an open research challenge [13], [18]. Cross-domain transfer learning offers a potential solution to data scarcity by enabling models trained in one environment to be adapted to others [15], [30], while domain adaptation techniques will be essential for managing distribution shifts across operational settings [8], [19]. Finally, standardization and benchmarking play a crucial role in enabling meaningful comparison of detection approaches [27], [29]. The development of community-driven datasets, evaluation protocols, and performance metrics will help accelerate progress in the field [26], [30]. Central to all these advancements is effective human–AI collaboration [10], [12]. Designing systems that complement human expertise, reduce cognitive burden, and support informed decision-making will be essential to maximizing the impact of AI in cybersecurity operations [14], [18].

VII. CONCLUSION

This study highlights the increasing importance of AI-based behavioral analytics in strengthening cybersecurity defenses against both known and unknown threats [2], [6]. An examination of recent research clearly demonstrates that behavioral analytics, when combined with modern machine learning techniques, significantly outperforms traditional signature-based and rule-driven security approaches [4], [19]. In particular, hybrid learning frameworks that integrate supervised, unsupervised, and semi-supervised methods consistently achieve higher detection accuracy, lower false-positive rates, and faster response times across a broad range of attack scenarios [6], [25], [30]. Deep learning models, including Long Short-Term Memory (LSTM) networks, autoencoders, attention-based architectures, and Graph Neural Networks, have shown strong effectiveness in modeling complex system behavior and identifying subtle, time-dependent attack patterns [9], [11], [21]. These approaches are especially well suited for detecting zero-day and stealthy attacks that frequently evade conventional security tools [4], [24]. When integrated with automated incident response mechanisms, they further enhance security operations by enabling faster alert generation, improved prioritization, and more efficient containment, thereby significantly reducing the time required for investigation and response [3], [12], [22].

The findings also indicate that AI-based behavioral analytics is highly adaptable and applicable across a wide range of cybersecurity domains, including network intrusion detection, cloud and containerized environments, Internet of Things (IoT) systems, industrial control systems, and insider threat detection [16], [18], [27]. Despite these strengths, several challenges remain. Limited availability of high-quality labeled data, vulnerability to adversarial attacks, lack of model transparency, high computational demands, and the complexity of real-world deployment continue to restrict broader adoption [7], [10], [28]. Looking forward, future research should prioritize the development of more explainable and robust detection models, privacy-preserving learning approaches such as federated learning, and lightweight solutions suitable for resource-constrained environments [1], [25]. Further exploration of reinforcement learning and Large Language Models for adaptive response orchestration and contextual threat intelligence also presents promising research directions [7], [22]. Overall, AI-based behavioral analytics represents a critical and evolving component of modern cybersecurity architectures, offering scalable, adaptive, and intelligent defenses capable of addressing the rapidly changing cyber threat landscape [18], [30].

VIII. REFERENCES

[1] Pal, "Agentic ai for proactive cyber-resilience in multi-cloud environments: Autonomous threat detection, response, and adaptive defense posturing," 2025. https://doi.org/10.38124/ijisrt/25jul1821

[2] Komarthi, "Ai-driven malware behavior analysis and threat prediction," International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences, 2025. https://doi.org/10.37082/ijirmps.v13.i4.232671

[3] Zhang, "Design and computational modeling of an ai-based automated cybersecurity incident response system," IEEE Access, 2025. https://doi.org/10.1109/access.2025.3603975

[4] "An adaptable deep learning-based intrusion detection system to zero-day attacks," Journal of Information Security and Applications, 2023. https://doi.org/10.1016/j.jisa.2023.103516

[5] Shaik, "Ai enhanced cyber security methods for anomaly detection," Learning and Analytics in Intelligent Systems, 2024. https://doi.org/10.1007/978-3-031-65392-6_30
[6] Kale, "A hybrid deep learning anomaly detection framework for intrusion detection," 2022. https://doi.org/10.1109/BigDataSecurityHPSCIDS54978.2022.00034
[7] Jaffal, "Large language models in cybersecurity: Applications, vulnerabilities, and defense techniques," arXiv.org, 2025. https://doi.org/10.48550/arxiv.2507.13629
[8] Nosakhare, "Machine learning in cybersecurity: A multi-industry case study analysis for enhanced threat detection and response," 2024. https://doi.org/10.51219/urforum.2024.victor-oriakhi-nosakhare
[9] Xu, "Tssan: Time-space separable attention network for intrusion detection," IEEE Access, 2024. https://doi.org/10.1109/access.2024.3429420
[10] Han, "Deepaid: Interpreting and improving deep learning-based anomaly detection in security applications," Computer and Communications Security, 2021. https://doi.org/10.1145/3460120.3484589
[11] Tang, "Zerowall: Detecting zero-day web attacks through encoder-decoder recurrent neural networks," International Conference on Computer Communications, 2020. https://doi.org/10.1109/INFOCOM41043.2020.9155278
[12] Aljumaily, "Enhancing user and entity behavior analytics in siem systems using ai-powered anomaly detection: A data-driven simulation approach," 2025. https://doi.org/10.33971/ijmrai.1.2.11
[13] Yuan, "Ada: Adaptive deep log anomaly detector," International Conference on Computer Communications, 2020. https://doi.org/10.1109/INFOCOM41043.2020.9155487
[14] Venkadesh, "Aegis ai - intelligent cyber resilience," Indian Scientific Journal Of Research In Engineering And Management, 2025. https://doi.org/10.55041/ijsrem42978
[15] Zhang, "Research progress on network security threat detection and defense technology based on artificial intelligence," Applied and Computational Engineering, 2025. https://doi.org/10.54254/2755-2721/2025.tj23838
[16] Makinde, "Ai-driven behavioral analytics for web application intrusion detection systems: A machine learning approach to anomaly detection."
[17] Husseini, "Advanced machine learning approaches for zero-day attack detection: A review." https://doi.org/10.1109/csnet64211.2024.10851751
[18] Bello, "The role of ai and machine learning in cybersecurity: Advancements in threat detection, anomaly detection and automated response," International Journal of Science and Research Archive, 2025. https://doi.org/10.30574/ijsra.2025.14.2.0542
[19] Carrasco, "A survey on deep learning for cybersecurity: Progress, challenges, and opportunities," Computer Networks, 2022. https://doi.org/10.1016/j.comnet.2022.109032
[20] Gupta, "The invisible defence: Detecting zero-day threats with ai."
[21] Li, "Anomaly-driven crypto-locking behavior analysis for ransomware detection through semantic flow mapping," 2024. https://doi.org/10.36227/techrxiv.173398043.39428308/v1
[22] Hmimou, "A multi-agent system for cybersecurity threat detection and correlation using large language models," IEEE Access, 2025. https://doi.org/10.1109/access.2025.3602681
[23] [23] Tuor, "Deep learning for unsupervised insider threat detection in structured cybersecurity data streams," 2017.
[24] [24] Hindy, "Utilising deep learning techniques for effective zero-day attack detection," 2020. https://doi.org/10.3390/electronics9101684
[25] Bahlali, "Self-supervised learning meets custom autoencoder classifier: A semi-supervised approach for encrypted traffic anomaly detection," IEEE Access, 2025. https://doi.org/10.1109/access.2025.3596179
[26] "Griffin: Real-time network intrusion detection system via ensemble of autoencoder in sdn," IEEE Transactions on Network and Service Management, 2022. https://doi.org/10.1109/tnsm.2022.3175710
[27] Jyothi, "Next-gen threat detection: Leveraging ai and cyber twin technologies for iot security," 2024. https://doi.org/10.1109/ssitcon62437.2024.10796384
[28] Wu, "Poison-resilient anomaly detection: Mitigating poisoning attacks in semi-supervised encrypted traffic anomaly detection," IEEE Transactions on Network Science and Engineering. https://doi.org/10.1109/tnse.2024.3397719
[29] "A hybrid multistage dnn-based collaborative idps for high-risk smart factory networks," IEEE Transactions on Network and Service Management, 2022. https://doi.org/10.1109/tnsm.2022.3202801
[30] Gudala, "Leveraging machine learning for enhanced threat detection and response in zero trust security frameworks: An exploration of real-time anomaly identification."