IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, November 2026
Impact Factor: 8.2

An Isolation Forest–Driven SOC Framework for Multi-Source Security Event Analysis and Human-Governed Automated Response

Gade Kuldeep Sunil, Doke Siddharth Mahesh, Kalekar Anuraj Santosh, Prof. Bhosale Sachin Bajirao
Dept. of Computer Engineering
Jaihind College of Engineering Kuran, India
gadekuldeep25@gmail.com, siddhudoke198@gmail.com,
kalekaranuraj@gmail.com, ssachinbhosale@gmail.com

Abstract : *Modern organizations generate large volumes of security events from servers, endpoints, firewalls, intrusion detection systems, and security applications. Traditional security monitoring mainly depends on predefined rules and manual investigation, which can result in alert fatigue, delayed response, and difficulty identifying abnormal behavior across multiple security sources. This research proposes an AI-Based Intrusion Detection System and Automated Response platform using Machine Learning and Security Orchestration, Automation and Response (SOAR). The proposed system collects and analyzes security events through Wazuh and integrates Snort, UFW, honeypot, and Gophish components to create a practical Security Operations Center (SOC) environment. Machine Learning, particularly Isolation Forest-based anomaly detection, is used to analyze security-event features and identify suspicious behavior. The system also performs attack classification, severity assessment, event correlation, and controlled automated remediation. A web-based SOC dashboard provides real-time monitoring of threats, attacker IPs, ML scores, firewall actions, and pending analyst reviews. To reduce the risk of incorrect automated blocking, critical responses can follow a Human-in-the-Loop workflow where analyst approval is required before sensitive actions. The proposed system aims to reduce alert-analysis effort, improve detection capability, and provide faster and safer incident response.*

Keywords: Intrusion Detection, Machine Learning, SOAR, Wazuh, Snort, Isolation Forest, SOC, Anomaly Detection, Automated Response, Cybersecurity, Threat Detection, Incident Response

I. INTRODUCTION

The increasing number of cyberattacks has made continuous security monitoring an important requirement for modern organizations. Servers, endpoints, firewalls, intrusion detection systems, applications, and other security tools continuously generate large amounts of security logs and alerts. Security Operations Center (SOC) analysts must examine these events, identify suspicious activities, correlate related alerts, determine the severity of incidents, and take appropriate response actions.

Traditional security monitoring systems primarily depend on predefined signatures, rules, and manual investigation. Although rule-based detection is effective for known attack patterns, it can generate a large number of alerts and may not effectively identify previously unseen or abnormal behavior. Security analysts therefore spend considerable time investigating false positives and correlating events from different security sources.

Machine Learning can assist security monitoring by identifying patterns and anomalies in collected security events. Anomaly detection techniques can identify behavior that differs from normal activity, while event features such as

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, November 2026 Impact Factor: 8.2

source IP, rule level, frequency, attack type, and repeated activity can be used for threat analysis. However, detection alone is not sufficient because security incidents also require timely response.

Security Orchestration, Automation and Response (SOAR) can connect detection with response actions through predefined playbooks. In this research, a practical SOC environment is developed using Wazuh, Snort, UFW, honeypot, and Gophish. Machine Learning is integrated with the detection pipeline to provide anomaly scoring and the SOAR layer is used to perform controlled remediation actions. The main objective is to improve threat detection and reduce response time while keeping the analyst involved in critical security decisions.

II. LITERATURE SURVEY

Several studies have investigated the use of Machine Learning, automated response, SOAR, and honeypot technologies for cybersecurity. Existing research focuses on improving detection accuracy, reducing false positives, identifying anomalous activities, and automating incident response. The following studies are closely related to the proposed system.

1. A. K. Aseres et al. (2026) proposed a systematic study of High-Interaction Honeypots (HIHPs) for cyber deception, focusing on their evolution, design, deployment, and future trends [1]. The study analyzed 163 papers, with 81 papers deeply evaluated, and introduced the HONEYLIFECYCLE Framework for standardized high-interaction honeypot lifecycle management and the Adaptive High-Interaction Honeypot (AHIH) Framework, which uses artificial intelligence and machine learning to dynamically engage threats. The study highlights the ability of honeypots to attract attackers and collect detailed information about their Tactics, Techniques, and Procedures (TTPs).

Limitation: High-interaction honeypots can be complex and resource-intensive to deploy, while proposed adaptive frameworks may require additional empirical validation. The proposed system uses honeypot-generated security events as one of the sources for centralized threat monitoring and analysis.

2. Racherla et al. (2024) proposed Deep-IDS, a real-time deep-learning-based intrusion detection system designed for resource-constrained IoT environments [2]. The system uses a simplified Long Short-Term Memory (LSTM) network containing 64 LSTM units and is trained using the CIC-IDS2017 dataset. It is deployed as an edge-server-based IDS positioned between IoT nodes and the Internet and is designed to detect Denial of Service (DoS), Distributed Denial of Service (DDoS), Brute Force, Man-in-the-Middle (MITM), and Replay attacks. The authors introduced an empirical threshold-selection approach to achieve a suitable trade-off between Detection Rate (DR) and False Alarm Rate (FAR). Deep-IDS achieved an overall classification accuracy of 97.67%, with precision of 97.67%, recall of 98.17%, and F1-score of 97.91%. It achieved a detection rate of 96.8% and required approximately 1.49 seconds on average to identify and mitigate intrusion attempts by blocking malicious traffic sources.

Limitation: The proposed system is specifically designed for IoT networks and uses a limited set of five attack categories. The authors also state that the system does not include countermeasures against Adversarial Machine Learning (AML) attacks, and the use of a Raspberry Pi 4 contributes to implementation cost. Our work will extend the intrusion-detection concept toward a broader SOC environment by analysing security events from multiple sources through Wazuh and integrating ML-based anomaly detection with controlled SOAR response and human approval for critical actions.

3. Satilmiş et al. (2024) presented a systematic literature review of Host-Based Intrusion Detection Systems (HIDS) by analysing research published between 2020 and 2023 [3]. The authors collected studies from academic databases including Scopus, Web of Science, IEEE Xplore, ScienceDirect, Springer Link, and ACM Digital Library and applied predefined selection and elimination criteria, resulting in 21 studies for detailed examination. The review analysed HIDS architectures, datasets, detection methods, evaluation metrics, and the advantages and disadvantages of Machine Learning and Deep Learning approaches. The study explains that HIDS primarily monitors host-level information such as system calls, DLL files, system logs, and registry keys, while anomaly-based HIDS can use ML/DL techniques to identify deviations from normal host behaviour. The review also examined passive and active response mechanisms, where active IDSs can automatically block or prevent detected attacks.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, November 2026 Impact Factor: 8.2

Limitation: The review identifies several limitations across existing HIDS research. A common issue is that many studies are evaluated mainly in laboratory environments rather than real-world environments. The review also highlights challenges associated with ML/DL-based anomaly detection, including large data requirements, training time, resource consumption, and the possibility of high false-alarm rates. The authors further identify the need for improved datasets and more realistic evaluation environments. Our work will address this practical gap by developing and testing an end-to-end SOC environment using real security logs and integrated security tools, combining anomaly detection, attack classification, alert correlation, and controlled automated response through SOAR.

4. J. Lee et al. (2025) proposed a Random Forest-based Intrusion Detection and Prevention System (RF-IDS) for Controller Area Network (CAN) bus communication in vehicles and implemented it as an Application-Specific Integrated Circuit (ASIC) using the TSMC 180 nm process [4]. The system applies a sliding window of 11 CAN identifiers to generate a 121-bit feature, uses five decision trees of depth nine with majority voting, and verifies the result through a rule-based filter for DoS, spoofing, and fuzzy attacks. When an attack is detected, the integrated CAN controller transmits an error frame to block the malicious node. The system achieved an average detection time of 1.86 µs, detection accuracy above 99% on the Car-Hacking dataset, and required only 4,437 LUTs on an FPGA.

Limitation: The model is a supervised classifier, so it may fail to identify new attack patterns that were not present during training, and it is limited to in-vehicle CAN networks. The authors suggest a hybrid cloud and on-device architecture to address unknown attacks. Our work uses unsupervised Isolation Forest-based anomaly detection to analyse security events from multiple sources and combines automated blocking with analyst approval.

5. J.-K. Lim et al. (2026) presented a smart-ship cybersecurity testbed that combines a digital twin of Electronic Chart Display and Information System (ECDIS) components with real-time threat detection and Security Orchestration, Automation and Response (SOAR) [5]. The testbed uses five maritime-specific playbooks and Kafka pipelines, and validates IACS UR E26 requirements with 85.7% (12/14) sub-requirement coverage. The evaluation reported a 91.8% overall detection rate (145/158 trials), a 100% SOAR playbook completion rate (500/500 executions), and a reduction of mean automated playbook completion time to 2.4 s compared with an estimated manual baseline of 348.0 s.

Limitation: The RECOVER phase is only partially covered (33.3%), the manual baseline was estimated rather than empirically measured, and the comparison with existing testbeds was scored from public documentation. The system is also specific to maritime operational technology. Our work applies the SOAR concept to a general SOC environment built with Wazuh, Snort, UFW, honeypot, and Gophish, and adds machine-learning scoring and human approval before sensitive actions.

6. T. Al-Shehari et al. (2023) proposed an insider threat detection model using the anomaly-based Isolation Forest algorithm to handle the highly imbalanced CERT r4.2 dataset, in which only 346 of 2,308,813 events are malicious [7]. Instead of oversampling or undersampling, the problem is handled at the algorithm level, and the contamination parameter was varied from 0.00 to 0.1. With a contamination ratio of 0.02, the model achieved 98% accuracy, 98% detection rate, and a 99% F-score, while supervised baselines such as Decision Tree, Random Forest, KNN, and XGBoost reached F-scores of only 66%, 37%, 36%, and 27%, respectively.

Limitation: Performance depends strongly on the contamination parameter, with accuracy dropping to 40% when it was set to 0, and the model was evaluated on a single synthetic dataset focused on data-leakage scenarios. The authors recommend further testing on different datasets. Our work applies Isolation Forest to real security events collected through Wazuh and adds attack classification, severity assessment, and controlled response.

7. K. Sadaf and J. Sultana (2020) proposed Auto-IF, a two-stage intrusion detection method for fog computing that combines an Autoencoder and Isolation Forest [8]. The autoencoder is trained only on normal traffic and separates normal and attack records using a reconstruction-loss threshold, after which two Isolation Forest modules correct the misclassified records in each set. Evaluated on the NSL-KDD dataset, the method achieved 95.4% accuracy, 94.81% precision, 97.25% recall, and a 96.01% F-measure, and performed better than the autoencoder used alone.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, November 2026 Impact Factor: 8.2

Limitation: The approach performs only binary classification of traffic as normal or attack, is validated on the older NSL-KDD benchmark, and requires tuning of the reconstruction-loss threshold and the contamination percentage. Our work extends anomaly detection with attack-type classification, event correlation, and SOAR-based response.

8. J. Zhang et al. (2025) proposed an AI-based Automated Incident Response (AIR) system to reduce the burden of alert volumes, reported as about 22,000 weekly alerts with approximately 68% false positives [9]. The system integrates STIX/TAXII-based multi-source log fusion, an attention-enhanced LSTM for temporal threat detection, a Bayesian game-theoretic decision layer, and a Deep Reinforcement Learning (DRL) validation module. It achieved a mean F1-score of 93%, an end-to-end latency of 58.3 ms, and a 39% reduction in false positives compared with threshold-based systems, with decisions that can be traced through STIX action chains and routed to manual review tickets when policy confidence is low.

Limitation: The architecture is computationally complex, was evaluated on NVIDIA A100 GPU servers, and was tested mainly on DDoS and command-and-control scenarios. The authors also state that its efficacy against AI-driven evasion requires further adversarial testing. Our work follows a lighter and more practical design that uses Isolation Forest scoring with a Human-in-the-Loop workflow for critical actions.

9. D. Shahjee and N. Ware (2022) presented a systematic analysis of the integration of Network Operation Centers (NOC) and Security Operation Centers (SOC) following the PRISMA methodology, with 75 articles selected for review [10]. The study defines an integrated NOC and SOC through people, process, and technology building blocks, and proposes a three-layer architecture consisting of a physical data source layer, an FCAPS/system management layer, and an overall situational management layer. It concludes that integration improves security posture, response time, and cost efficiency, while identifying limited integrated tools, insufficient automation, and the lack of defined standards as major challenges.

Limitation: The work is conceptual and literature-based and does not provide an implemented or experimentally evaluated system. Our work provides a practical SOC laboratory implementation that centralizes security monitoring, ML-based analysis, and automated response.

10. M. A. M. Farzaan et al. (2025) proposed an AI-powered cyber incident detection and response system for cloud environments that integrates network traffic classification, a web intrusion detection system, and post-incident malware analysis [11]. The system is implemented as a containerised Flask application compatible with Google Cloud and Microsoft Azure. Using the NSL-KDD, UNSW-NB15, and CIC-IDS-2017 datasets, the Random Forest model achieved accuracies of 90%, 75%, and 99%, respectively, while malware analysis reached 96% precision and a neural network model reached 99% accuracy.

Limitation: Detection accuracy varies considerably between datasets, particularly for UNSW-NB15 (75%), and the system relies mainly on supervised models trained on public datasets. Our work focuses on analysing live security events from Wazuh, Snort, UFW, honeypot, and Gophish through unsupervised anomaly scoring and controlled SOAR response.

11. M. Vielberth et al. (2020) conducted a systematic study of Security Operations Centers (SOCs) to establish a generally accepted definition and identify the primary building blocks of a SOC in terms of people, processes, technologies, and governance and compliance [21]. The study also summarizes open challenges and notes that academic research focuses mainly on human and technological aspects while neglecting the processes that connect them. It highlights that the mean time to detect an incident was 196 days, with an additional 69 days required for containment.

Limitation: The study is a literature survey and does not propose an implemented detection or response system. Our work addresses the process gap by implementing a complete pipeline from event collection to detection, incident creation, controlled remediation, and analyst review.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, November 2026
Impact Factor: 8.2

III. EXISTING SYSTEM

Existing cybersecurity monitoring environments commonly use individual security tools such as firewalls, IDS/IPS solutions, SIEM platforms, and endpoint monitoring systems. These tools can generate security alerts when predefined signatures, rules, or thresholds are triggered. However, the generated alerts often require manual investigation by SOC analysts. Traditional systems generally treat security events independently, making it difficult to correlate repeated activity from the same source across different security tools. Large numbers of alerts can result in alert fatigue and increase the possibility of delayed incident response. Rule-based systems may also have difficulty identifying abnormal behavior that does not match predefined signatures.

Some modern security platform provide automated response capabilities, but fully automated blocking can create operational risk when an alert is incorrectly classified. Blocking a legitimate source can affect business services and users. Therefore, there is a need for a system that combines centralized security monitoring, Machine Learning-based anomaly detection, event correlation, and controlled automated response.

The proposed system addresses these limitations by combining Wazuh, Snort, UFW, honeypot, Gophish, Machine Learning, and SOAR into a single SOC-oriented environment.

IV. PROPOSED SYSTEM

The proposed system is an AI-Based Intrusion Detection and Automated Response platform designed to assist SOC analysts in detecting, investigating, and responding to cyber threats. Security events are collected from multiple sources, including Wazuh and integrated security components such as Snort, firewall activity, honeypot events, and simulated phishing activity.

Wazuh acts as the central security monitoring component and provides structured security alerts containing information such as rule identifiers, rule levels, descriptions, source IP addresses, agents, timestamps, and attack-related metadata. These events are processed by the Machine Learning pipeline to identify abnormal behavior.

The implemented Machine Learning engine uses Isolation Forest for anomaly detection. Security events are transformed into relevant features and analyzed to generate an anomaly score. The system also uses sliding-window aggregation to identify repeated activity from an attacker IP within a defined time period. This helps identify behavioral patterns such as repeated authentication failures, scanning activity, directory enumeration, and other repeated security events.

The detection pipeline assigns severity based on the ML anomaly score and security-event characteristics. Attack activity can be classified into categories such as brute-force activity, SQL injection, credential spraying, rootkit behavior, ransomware behavior, unusual SSH activity, directory enumeration, XSS, and command injection based on available event information.

After detection and analysis, the SOAR layer performs controlled response actions. The remediation component validates attacker IP addresses and applies safeguards such as response debouncing and simulation controls before firewall actions are performed. The system supports blocking and unblocking of suspicious IP addresses and maintains incident information for analyst review.

A web-based SOC Command Center provides real-time visibility into detected threats, automated firewall blocks, pending SOC reviews, unique attacker IP addresses, ML scores, severity levels, attack categories, and event activity. WebSocket-based communication allows security events and dashboard information to be updated in real time.

An important component of the proposed architecture is the Human-in-the-Loop approach. Critical security decisions are not intended to depend only on an ML score. Instead, sensitive actions can be presented to the SOC analyst for approval. This reduces the possibility of legitimate users or systems being incorrectly blocked while still allowing routine security responses to be automated.

The complete system therefore creates a pipeline from security-event collection → detection → feature analysis → anomaly scoring → attack/severity analysis → incident creation → controlled remediation → SOC analyst review → monitoring.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, November 2026
Impact Factor: 8.2

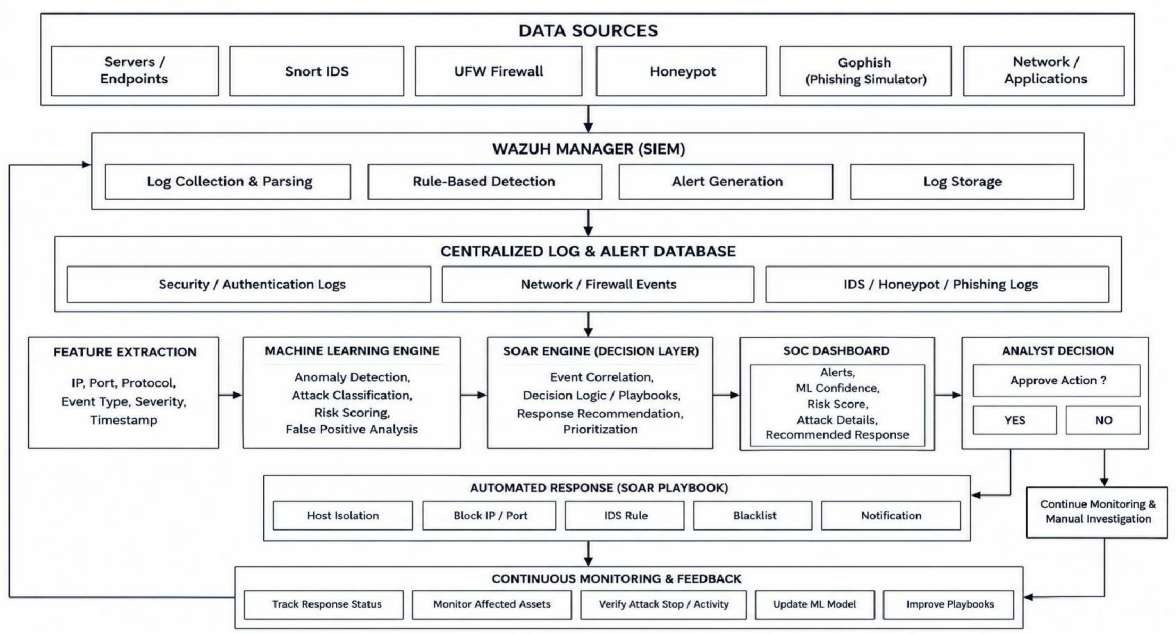


Figure 1 : Initial Work Flow Diagram for Explaining the actual working in blocks

V. FUTURE SCOPE

- Automatic mapping of detected activities to MITRE ATT&CK techniques and tactics.
- Integration with additional SIEM and SOAR platforms.
- Advanced Threat Intelligence integration for IP, domain, URL, and file reputation analysis.
- Improved Machine Learning models for attack classification and behavioral detection.
- Continuous model retraining using validated SOC analyst feedback.
- Advanced correlation of events from multiple security sources.
- Development of additional automated response playbooks.
- Integration of YARA and malware-analysis capabilities.
- Advanced phishing and social-engineering detection using the Gophish environment.
- Expansion toward distributed SOC monitoring and real-time threat hunting.

VI. CONCLUSION

The proposed AI-Based Intrusion Detection System and Automated Response platform combines centralized security monitoring, Machine Learning, and SOAR capabilities to improve cybersecurity detection and response. Wazuh provides security-event monitoring, while Snort, UFW, honeypot, and Gophish contribute additional security telemetry. Isolation Forest is used for anomaly detection and behavioral analysis, while the SOAR layer provides controlled remediation and analyst workflows.The web-based SOC dashboard provides real-time visibility into threats, attacker activity, ML scores, firewall actions, and pending investigations. By incorporating Human-in-the-Loop approval for sensitive actions, the system aims to balance automation with operational safety. Overall, the proposed platform provides a practical SOC laboratory architecture for detecting suspicious behavior, correlating security events, and reducing the time required to respond to cyber incidents.Detect intelligently. Respond automatically. Monitor continuously.

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/IJARSCT-40740

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, November 2026
Impact Factor: 8.2

REFERENCES

[1] A. K. Aseres, S. Z. Melese, A. M. Beyene, and L. K. Tegegne, "High-Interaction Honeypots in Cyber Deception: Evolution, Design, Deployment, and Future Trends," IEEE Access, vol. 14, pp. 99861–99896, 2026, doi: 10.1109/ACCESS.2026.3706613.

[2] S. Racherla, P. Sripathi, N. Faruqui, M. A. Kabir, M. Whaiduzzaman, and S. A. Shah, "Deep-IDS: A Real-Time Intrusion Detector for IoT Nodes Using Deep Learning," IEEE Access, vol. 12, pp. 63584–63597, 2024, doi: 10.1109/ACCESS.2024.3396461.

[3] H. Satılmış, S. Akleylek, and Z. Y. Tok, "A Systematic Literature Review on Host-Based Intrusion Detection Systems," IEEE Access, vol. 12, pp. 27237–27266, 2024, doi: 10.1109/ACCESS.2024.3367004.

[4] J. Lee, S. Park, S. Shin, H. Im, J. Lee, and S. Lee, "ASIC Design for Real-Time CAN-Bus Intrusion Detection and Prevention System Using Random Forest," IEEE Access, vol. 13, pp. 129856–129869, 2025, doi: 10.1109/ACCESS.2025.3585956.

[5] J.-K. Lim, H.-S. Song, J.-W. Kim, and Y.-H. Choi, "A Digital Twin and SOAR-based Cybersecurity Testbed for Automated Threat Detection and Response in Smart Ships," IEEE Access, 2026, doi: 10.1109/ACCESS.2026.3735911.

[6] J. Lee, S. Park, S. Shin, H. Im, J. Lee, and S. Lee, "ASIC Design for Real-Time CAN-Bus Intrusion Detection and Prevention System Using Random Forest," IEEE Access, vol. 13, pp. 129856–129869, 2025, doi: 10.1109/ACCESS.2025.3585956.

[7] T. Al-Shehari, M. S. Al-Razgan, T. Alfakih, R. A. Alsowail, and S. Pandiaraj, "Insider Threat Detection Model Using Anomaly-Based Isolation Forest Algorithm," IEEE Access, vol. 11, pp. 118170–118185, 2023, doi: 10.1109/ACCESS.2023.3326750.

[8] K. Sadaf and J. Sultana, "Intrusion Detection Based on Autoencoder and Isolation Forest in Fog Computing," IEEE Access, vol. 8, pp. 167059–167068, 2020, doi: 10.1109/ACCESS.2020.3022855.

[9] J. Zhang, S. Li, W. Huang, H. Jing, Q. Zhang, and X. Xia, "Design and Computational Modeling of an AI-Based Automated Cybersecurity Incident Response System," IEEE Access, vol. 13, pp. 154383–154394, 2025, doi: 10.1109/ACCESS.2025.3603975.

[10] D. Shahjee and N. Ware, "Integrated Network and Security Operation Center: A Systematic Analysis," IEEE Access, vol. 10, pp. 27881–27898, 2022, doi: 10.1109/ACCESS.2022.3157738.

[11] M. A. M. Farzaan, M. C. Ghanem, A. El-Hajjar, and D. N. Ratnayake, "AI-Powered System for an Efficient and Effective Cyber Incidents Detection and Response in Cloud Environments," IEEE Transactions on Machine Learning in Communications and Networking, vol. 3, pp. 623–643, 2025, doi: 10.1109/TMLCN.2025.3564912.

[12] M. Khayat, E. Barka, M. A. Serhani, F. M. Sallabi, K. Shuaib, and H. M. Khater, "Empowering Security Operation Center With Artificial Intelligence and Machine Learning—A Systematic Literature Review," IEEE Access, vol. 13, pp. 19162–19197, 2025, doi: 10.1109/ACCESS.2025.3532951.

[13] D. Benka, D. Horváth, L. Špendla, G. Gašpar, and M. Strémy, "Machine Learning-Based Detection of Anomalies, Intrusions, and Threats in Industrial Control Systems," IEEE Access, vol. 13, pp. 12502–12514, 2025, doi: 10.1109/ACCESS.2025.3530902.

[14] W. Dai, X. Li, W. Ji, and S. He, "Network Intrusion Detection Method Based on CNN-BiLSTM-Attention Model," IEEE Access, vol. 12, pp. 53099–53111, 2024, doi: 10.1109/ACCESS.2024.3384528.

[15] S. Elsayed, K. Mohamed, and M. A. Madkour, "A Comparative Study of Using Deep Learning Algorithms in Network Intrusion Detection," IEEE Access, vol. 12, pp. 58851–58870, 2024, doi: 10.1109/ACCESS.2024.3389096.

[16] M. Azhar, S. Perveen, A. Iqbal, and B. Lee, "IDRandom-Forest: Advanced Random Forest for Real-Time Intrusion Detection," IEEE Access, vol. 12, pp. 113842–113854, 2024, doi: 10.1109/ACCESS.2024.3443408.

[17] M. Cantone, C. Marrocco, and A. Bria, "Machine Learning in Network Intrusion Detection: A Cross-Dataset Generalization Study," IEEE Access, vol. 12, pp. 144489–144508, 2024, doi: 10.1109/ACCESS.2024.3472907.

[18] S. A. Abdulkareem, C. H. Foh, M. Shojafar, F. Carrez, and K. Moessner, "Network Intrusion Detection: An IoT and Non IoT-Related Survey," IEEE Access, vol. 12, pp. 147167–147191, 2024, doi: 10.1109/ACCESS.2024.3473289.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, November 2026
Impact Factor: 8.2

[19] J. Saikam and K. Ch, "EESNN: Hybrid Deep Learning Empowered Spatial–Temporal Features for Network Intrusion Detection System," IEEE Access, vol. 12, pp. 15930–15945, 2024, doi: 10.1109/ACCESS.2024.3350197.
[20] O. Arreche, I. Bibers, and M. Abdallah, "A Two-Level Ensemble Learning Framework for Enhancing Network Intrusion Detection Systems," IEEE Access, vol. 12, pp. 83830–83857, 2024, doi: 10.1109/ACCESS.2024.3407029.=
[21] M. Vielberth, F. Böhm, I. Fichtinger, and G. Pernul, "Security Operations Center: A Systematic Study and Open Challenges," IEEE Access, vol. 8, pp. 227756–227779, 2020, doi: 10.1109/ACCESS.2020.3045514.