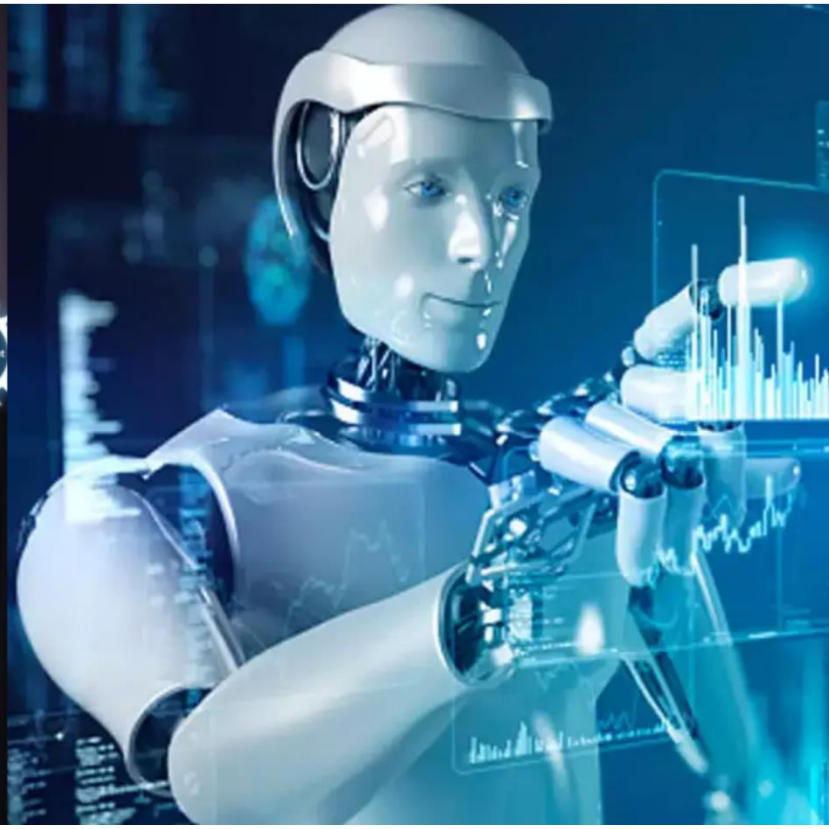
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 11, November 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411086|

AI-Driven Threat Hunting: Leveraging Machine Learning for Proactive Threat Detection and Incident Response

Vaibhav Hariramani

Student, BITS Dubai Campus, Dubai, UAE

ABSTRACT: The paper explores the role of Artificial Intelligence (AI) and Machine Learning (ML) in proactive threat hunting and incident response in cybersecurity processes. Based on secondary data through the Google Scholar, it reviews literature on five topics, including the development of threat hunting, machine learning methods in detection, real-time analysis and automation, interpretability and robustness, and deployment issues with ethical considerations. The results demonstrate that threat hunting with AI plays a major role in enhancing the speed and accuracy of defence in the case of anomaly detection, prediction, and automated response. Nevertheless, the problems of interpretability, adversarial manipulation, concept drift, and ethical responsibility are significant obstacles to operational implementation. The paper presents the necessity of explainable, resilient, and ethically controlled AI systems with the ability to balance automation and human control. On the whole, the study emphasizes that although AI can bring revolutionary benefits to cybersecurity, ongoing cooperation, transparency, and flexibility between technology and manual skills are the only means of sustainable success.

KEYWORDS: Artificial Intelligence (AI); Machine Learning (ML); Threat Hunting.

I. INTRODUCTION

In the current interconnected digital environment, the cyber threats are more advanced and inescapable than ever before. Conventional signature-based defenses that have been based on a set of set rules and known attack patterns, are becoming less effective in keeping up with new adversarial behaviors, including zero-day exploits, rogue lateral movement and sophisticated persistent threats (Ali and Kostakos, 2023). This leads to the fact that enterprises are moving towards active defence, and threat hunting has become one of the main support pillars. Threat hunting is an active search of the networks, looking for strongholds in them, not the response to an indicator of intrusion (Edmund and Enemosah, 2024).

It is against this background that there has been an opportunity of convergence of the artificial intelligence (AI) and machine learning (ML). With constant consumption of large amounts of telemetry (network flows, endpoint logs, user behaviour, threat intelligence feeds, etc.), ML models have been shown to identify subtle behavioral changes, train behaviour changes over time, and provide real-time alerts to incident responders (Blessing Guembe et al., 2025). These systems are also able to adjust to new threat surface unlike the fixed rule engines and contribute to minimizing the detection latency and analyst burden. In fact, AI-assisted threat hunting is becoming a new strategic direction of cybersecurity that allows organisations to detect threats before they develop causing organisations to automate routine processes and enhance the effectiveness of responding to an incident. The paper explores the ways in which pipelines built with ML can be used to facilitate anomaly detection in real-time, predictive analytics, and automated response playbooks - eventually leading to more resilience in the operations of a contemporary security operation (editorialteam, 2025).

II. RATIONALE AND OBJECTIVE

Rationale

The fast rise in cyberattacks, data breaches, and zero day exploits point to the inefficiency of traditional security systems which are based on static rules and human surveillance. Traditional intrusion detection equipment has been shown to fail in detecting advanced or uncharacterised threats, and thus resulting in slow reaction and expensive loss. The introduction of Artificial Intelligence (AI) and Machine Learning (ML) has become a potent answer to this gap, as

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411086|

it allows proactive, automated, and adaptive threat hunting (Gupta, 2022). ML algorithms are able to process large and complicated data streams in real-time and identify abnormal behaviour patterns and forecast possible breaches before they happen. Implementing AI in the threat-hunting operations does not only improve accuracy and speed, but it also lowers the fatigue of the analysts and increases the efficiency of the incident response. The study is thus important in that it discusses the way AI-based systems can turn cybersecurity into an active defence rather than a reactive one (Merlano, 2024).

Objectives

1. To analyze the ways AI and ML models can be used to facilitate active identification of sophisticated and dynamic cyber threats.
2. To compare the performance and reliability of various ML algorithms in real time anomaly detection and incident response.
3. To suggest a workable model of implementing AI-based threat-hunting systems within current security processes to enhance the detection rate and decrease response time.

III. METHODOLOGY

This paper is founded on only secondary data sources gathered via the Google scholar database that is the main source of peer-reviewed and academic literature. The keywords (AI in cybersecurity, machine learning threat detection, and automated incident response) were used to find the relevant journal articles, conference papers, and review studies that related to Artificial Intelligence (AI), Machine Learning (ML), and cybersecurity threat hunting. Articles that were published between 2015 and 2025 were given priority to facilitate the incorporation of relevant and reliable results.

The method of review, interpretation, and comparison of the selected studies was discussed using a qualitative content analysis approach. The literature review was critically assessed to determine general trends, approaches, advantages, and drawbacks of AI-based threat detection and action systems.

During the research, ethical considerations were strictly observed. No intellectual property or academic dishonesty were violated using only publicly available and well-referenced sources. No personal, confidential and sensitive information was accessed or duplicated. The research also recognizes the ethical significance of transparency, fairness and not being biased when interpreting the secondary information.

With this methodology, the research will remain ethical, verifiable and based on credible scholarly knowledge of Google Scholar.

IV. LITERATURE REVIEW

1. Threat Hunting Evolution and the Machine Learning

The practice of threat hunting is becoming more accepted as an active form of cybersecurity, in which threats are actively sought in networks prior to the activation of automated warning mechanisms or intrusion detection software (Ndayipfukamiye et al., 2025). Threat hunting is in contrast to traditional reactive security mechanisms, which rely heavily on predefined signatures or rule-based detections in the context of uncovering unknown or stealthy adversarial behaviour by means of hypothesis-based exploration and behavioural analysis. As recent reviews of threat hunting research show, the concept has become the focus of academic and industrial attention by around 2016, being a big change to reactive incident response, to proactive defensive tactics (Olaoye, 2025).

More complex attacks (including zero-day exploits, insider threats, and advanced persistent threats (APTs)) have been known to defeat conventional systems, including signature-based intrusion detection and static rule engines. Such constraints have encouraged scholars and practitioners to incorporate Artificial Intelligence (AI) and Machine Learning (ML) into the threat-hunting practice (Nwaodike, 2025). ML algorithms can analyze large and complicated data sets, including network traffic, system logs, and user behaviour, much more efficiently and quickly than hand analysis. This will help them to identify minor anomalies, understand changing attacker behaviours, and deliver predictive intelligence instead of mere alerting.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411086|

According to various studies, sub-trends in this evolution include the replacement of the manual investigation with the automated one, the proliferation of the source of telemetry, and the growing need of the scalability of large enterprise networks (Onih, Sevidzem and Adeniji, 2024). ML-driven systems provide flexibility in that they constantly learn with new data and increase their accuracy at detecting it. Nevertheless, the literature also cautions that operationalising ML-based threat hunting is not an easy task because of the problems related to data quality, labelling challenges, model drift, and using human analysts in the loops of making a decision (Priyadharshini et al., 2025).

On the whole, this theme predetermines that AI-based threat hunting is a logical and timely development in the sphere of cybersecurity. With threat actors becoming more dynamic and unpredictable, scalable, adaptive, and proactive defence with the help of ML can be used to effectively predict and counter attacks before they can inflict damage (Pillai, 2023).

2. Threat detection by use of Machine Learning

The scope of a research on the topic of AI-driven threat hunting is expanding as a variety of methods of Machine Learning (ML) is studied that are the basis of this field. They are supervised, unsupervised, semi-supervised, deep learning, reinforcement learning as well as hybrid or ensemble models that offer distinct benefits to proactive cyber defence (Rahmati, 2025).

The algorithms are trained using the labelled data in supervised learning to identify known attack patterns. Random Forest, Support Vector Machines (SVM), Logistic Regression, and AdaBoost are frequently used models to detect intrusions because it is easy to interpret and because of accuracy (Reddy Kethireddy, 2022). An example of this is a recent study of the critical infrastructure security where the AdaBoost algorithm was found to produce more than 95 percent detection accuracy and a ROC with an area of 0.98 in distinguishing between normal and abnormal network traffic. These models are effective in case there are full data sets that are balanced and labelled (Konakanchi, 2025)
Nevertheless, laboratory data is frequently restricted in the field of actual cybersecurity. Thus, unsupervised and semi-supervised methods of learning, including Autoencoders, Isolation Forests, and K-means clustering, have been essential in detecting anomalies (reddit.com, 2025). These models detect abnormal behaviour without any prior understanding of attack signature, and they are effective especially in detection of zero-day attack or new threats.

Deep learning with convolutional neural networks (CNNs) to identify traffic patterns and long short-term memory (LSTM) or Gated Recurrent Unit (GRU) to analyse sequential system or network logs have further enabled threat detection. In the meantime, reinforcement learning is becoming a promising means of adaptive defence where systems are able to change their detection strategies dynamically in response to changing attack behaviours (Aiswarya, 2021).
Finally, hybrid and ensemble models are more robust as they utilize the benefits of a variety of learning strategies, which minimizes false positives and concept drift (Reddy Kethireddy, 2022). There is evidence that mixed groupings of deep and shallow learners outperform generalisation and flexibility in multi-volume network settings.

Overall, the literature keeps on noting that the choice of model is determined by data quality, the level of threat, urgency of the operations, and operational restrictions, and there cannot be one universal best ML method that can be highly effective in all threat-hunting scenarios (Edris, 2025).

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

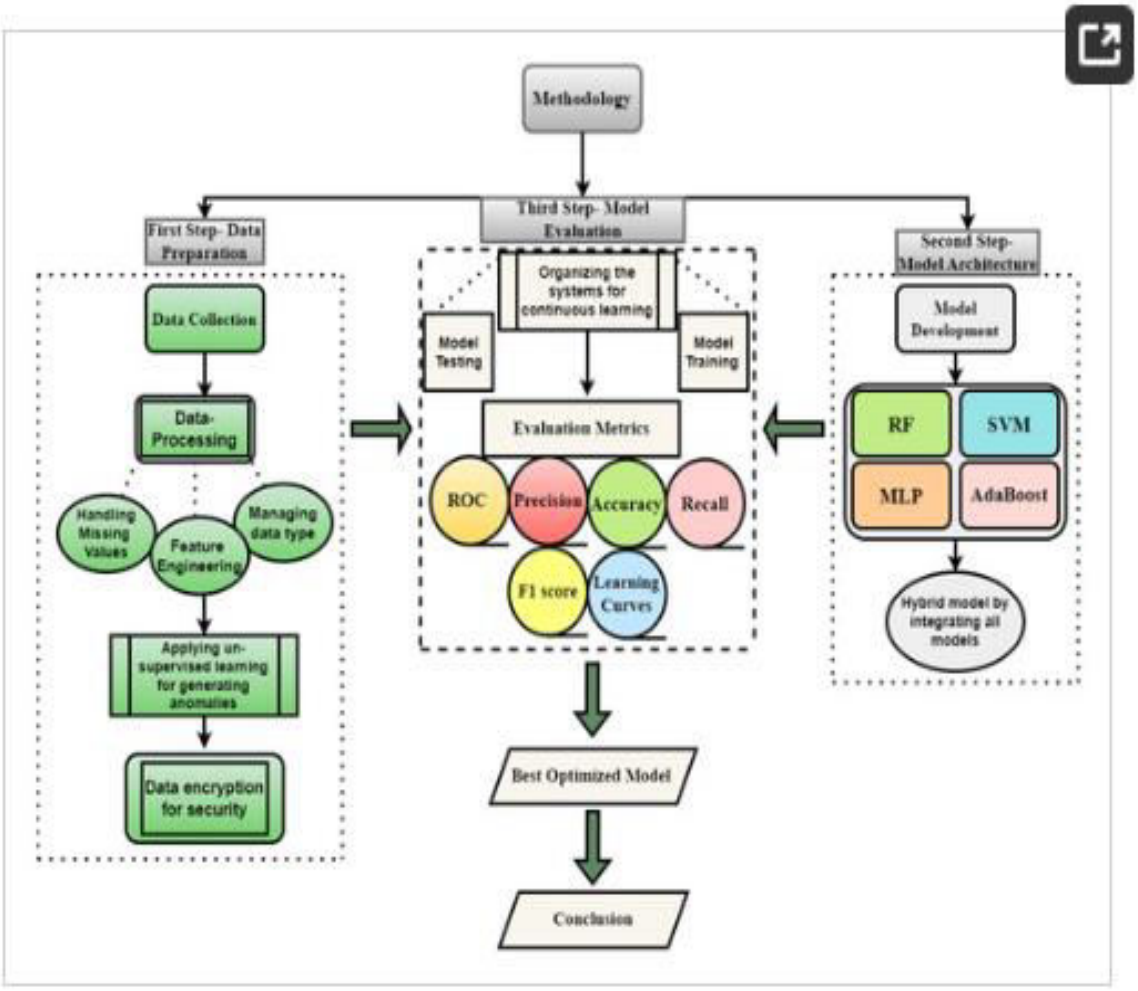
|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411086|

3. Incident Response (320 words) Real-Time Analysis, Anomaly Detection, and Automation

Flow chart of the methodology used for cyber-attack detections



(Shan and Seunghwan Myeong, 2024)

The third significant theme discusses the role of the Artificial Intelligence (AI) and Machine Learning (ML) in changing real-time analysis, anomaly detection, and automation as part of the cybersecurity incident response model. In threat hunting of the present day, detection is not the goal, but low-latency identification and the ability to respond quickly to minimize possible harm. Recent research highlights the importance of real-time or near-real-time detection of the threats to counter the rapidly changing cyberattacks (Sewak, Sahay and Rathore, 2022).

Proactive defence is still based on anomaly detection. ML models constantly observe network, host, and user activity to detect the deviation of the established baselines. Such anomalies may signal insider threats, credentials attacks, or cunning lateral motions (Savadatti et al., 2024). Nonetheless, scholars have reported the following issues to persist indefinitely: high rates of false positives, understanding alerts and limited computation ability to sustain accuracy at scale. There are attempts to optimise algorithms of contextual comprehension and prioritisation of real dangers.

Automation is a complementary tool whereby it is used to tie ML-driven detection systems with Security Orchestration, Automation, and Response (SOAR) systems and incident response (IR) playbooks. With this integration, it becomes automatic to execute such containment steps as isolating infected endpoints, blocking

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411086|

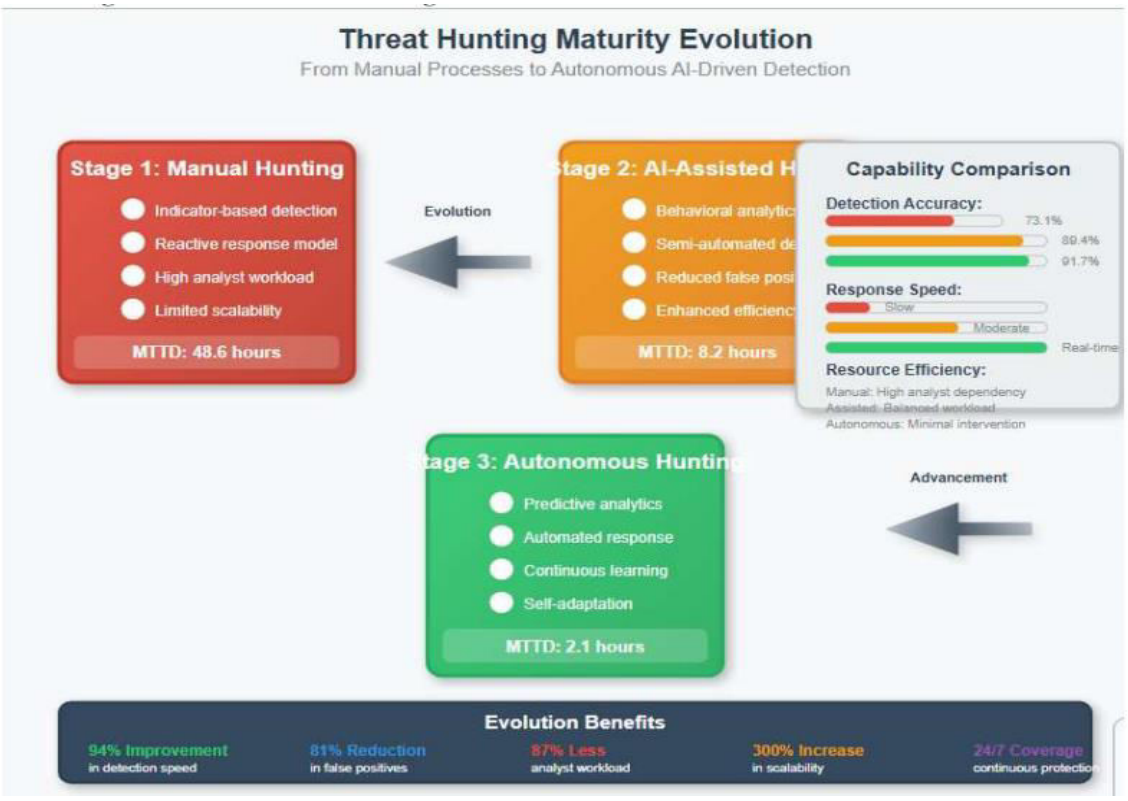
malicious IP addresses, or forwarding incidents to analysts (Shan and Seunghwan Myeong, 2024). AI-enhanced automation decreases the time between detection and response, increases accuracy and decreases man work in Security Operations Centres (SOCs).

However, the application of ML models to real-time environments presents such challenges as streaming data processing, concept drift (the development of behavioural norms with time), and resource constraints on edge or Internet of Things (IoT) devices. Newer investigations support the use of Explainable and Lightweight AI models to achieve operational viability and confidence in automated systems (Thaqi et al., 2024).

In general, this theme highlights how the industry is moving away offline, batch-based analytics towards continuous and integrated monitoring systems, incorporating detection, alerting and automated response, and the next step in this direction is intelligent, self-defending networks.

4. Interpretability, Adversarial Robustness, and Concept drift

One of the most important but minimally discussed aspects of AI-enhanced threat hunting entails three closely interconnected issues, namely interpretability, adversarial strength, and concept drift. These aspects define the possibility of keeping Machine Learning (ML) models transparent, trustful, and reliable in changing cybersecurity contexts (Ali and Kostakos, 2023).



(Nwaodike, 2025)

Interpretability is also an emerging fear because most ML models, especially deep neural networks, are black-box models. When an alert is raised by a model that an analyst cannot comprehend why that model had been showing the alert (Blessing Guembe et al., 2025). The literature emphasizes that explainability is not only desirable, but also critical to the trust and accountability among analysts and their adoption of operations. To overcome this, studies of Explainable AI (XAI) have presented interpretability methods including SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations) that assist in visualising and justifying model choices (Gupta, 2022). A new project, HuntGPT, is an anomaly detection system that uses MLs along with Large Language

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411086|

Models (LLMs) and XAI to provide human-readable justifications to alerts, making transparency improvements (Mackay, 2024).

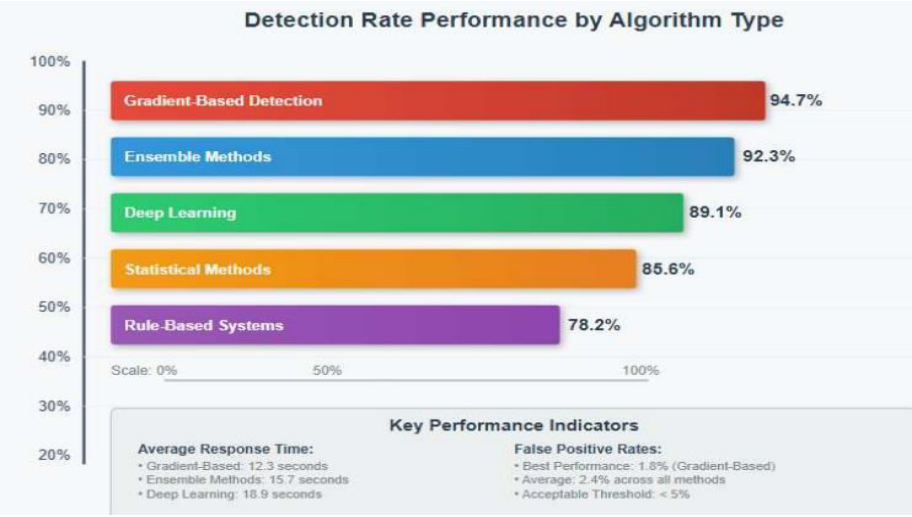
Another urgent problem is adversarial robustness. Adversarial evasion Attackers can manipulate inputs and mislead ML to commit adversarial evasion, or can corrupt training data to corrupt model training (Merlano, 2024). There is a systematic review on Generative Adversarial Networks (GANs) in cybersecurity that because AI can be used as a defense mechanism, it can also create vulnerabilities, and therefore stable and resistant models against data manipulation are important. Finally, concept drift is the change in data distribution due to the change in network behaviour, user behaviour and attack strategies. In a typical Security Operations Centre (SOC), the real world situation requires the use of static models that rapidly degrade unless they are retrained or updated in an adaptive manner. To be able to keep performance stable, adaptive learning pipelines and online retraining have been suggested (Razavi et al., 2025).

Finally, the literature emphasizes that to ensure sustainability of AI-based threat hunting, interpretability, robustness, and adaptability should be incorporated into the model development, such that not only accuracy is ensured, but also resilience and trust in live cybersecurity search (Ndayipfukamiye et al., 2025).

5. Deployment Problems, Ethical Implications and Future Projections

The last theme is the operational, ethical, and future research issues in the context of the implementation of AI-driven threat hunting in the real-life cybersecurity setting. Although there are great strides in the area of research, implementation is complicated and resource intensive. The major operational challenges are the quality and quantity of data, integration with the existing security infrastructure, e.g., SIEM, EDR, and SOAR systems, scalability, cost, and the constantly existing cybersecurity skills gap (Nwaodike, 2025). Researchers emphasize that false positives, data reliance, and interpretation of models remain the main obstacles to the successful adoption, as opponents actively create methods to avoid or abuse AI systems.

The concerned ethical issues are becoming more observable in literature. Monitoring AI systems that identify abnormal user behaviour is an issue of privacy especially when it comes to constant data gathering and tracking (Algabri, 2025). Other concerns include biases in algorithms, in which models can end up rewarding specific behavioural norms unintentionally and accountability, in which the question of responsibility concerning automated security decisions is not evident. Being transparent and fair is vital in ensuring the stakeholder trust (Onih, Sevidzem and Adeniji, 2024). Also, the researchers and practitioners warn against excessive automation; and insist that human control and human-computer cooperation are also crucial to avoid any errors and to have ethical control.



(Nwaodike, 2025)

Regarding the future directions, there are a number of priorities that are emerging both in academic and practitioner research:

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411086|

- Establishing unified benchmarks and metrics of evaluation to enhance comparability of AI threat-detection models.
- Enhancing lightweight and edge-capable ML, IoT, and distributed (Rahmati, 2025).
- Enhancement of adversarial defences: GAN-based architecture and resilient architecture.
- Combining cyber threat intelligence (CTI) and ML pipelines to achieve dynamic and context-aware adaptation (Al-Sawwa, 2025).
- Vindicating human-in-the-loop constructions, making SOC workflow explainable and with measurable work performance.

In short, even though AI holds a potentially transformative potential of improving proactive and intelligent threat hunting, the ethical, interpretable and livable deployment of AI in live operational environments is still a persistent research and application dilemma (Reddy Kethireddy, 2022).

Generalization and Research implications

Combining the five themes, the literature provides the dynamic and complex image of the AI-powered threat hunting- a domain that is rapidly growing in technological terms; has an increasing technical complexity; and is facing continuous practical and ethical issues. All these in combined effect exemplify how Machine Learning (ML) and Artificial Intelligence (AI) have enabled cybersecurity to be moved to reactive detection to proactive, predictive, and automated defence mechanisms.

Themes 1-3 determine that AI and ML play an important role in improving threat detection, anomaly identification, and automation of real-time responses . The transformation of signature-based detection to behaviour-based and adaptive learning techniques has enhanced the speed and accuracy of detection of known and unknown threats. Yet, the literature also acknowledges that these technological developments should be supported by operational preparedness and human-in-the-loop style in order to make contextual decisions.

Theme 4 brings out more structural issues involving interpretability, adversarial robustness and concept drift. Deep and ensemble models may be better than the traditional ones, but they are black-box, and this quality can be concerning in terms of trust, explainability, and reliability. Moreover, with adversarial manipulation and changing patterns in data, constant retraining and observation of the model is needed to ensure that information is relevant in real-time.

Theme 5 builds up on this discussion to realities of deployment, ethics and future research directions. The main obstacles to implementation include breaking integration walls, making the models transparent, protecting privacy, and minimizing the bias of the algorithms. The new agreement points out that the concept of human supervision, responsibility, and ethical regulation should still play an important role in AI implementation in cyberspace security.
In the case of research, these findings indicate that technical performance is not enough. Future research needs to consider frameworks that strike a balance between the accuracy of detection and its interpretability, automation, and human judgement and innovation versus ethical accountability. The gaps identified by the researchers to include the absence of standardised evaluation criteria, small-scale studies of the real-world deployment, and ad inconsistent application of explainability methods are challenged to enhance the academic and operational plausibility.

V. CONCLUSION

The review concludes that AI-based threat hunting, which is driven by the power of Machine Learning (ML), is redefining contemporary cybersecurity by allowing to detect threats proactively, respond to incidents faster and predict defence. Combining the use of supervised, unsupervised and deep learning models enable security systems to detect subtle anomalies and emerging threats that are mostly ignored by traditional methods. However, as it has always been demonstrated in the literature, the problem of transferring these technical advances to real life activities is still a formidable challenge.

In addition to the performance of the algorithms, interpretability, robustness, and adaptability are the long-term successful factors of AI-based systems. Trust and reliability may be compromised by black-box models, adversarial manipulation, concept drift, etc. unless treated properly. Moreover, ethical aspects: privacy, accountability, and

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411086|

fairness need more focus especially with more control being taken over by automated systems in Security Operations Centres (SOCs).

The future studies should thus be focused on creating explainable, resilient and ethically responsible AI structures that fuse with human expertise. The need to have unified benchmarks, improve adversarial defences and continuous learning will be critical towards operational sustainability. Finally, even though AI shows significant transformative potential in relation to cybersecurity, its implementation will have to be dominated by transparency, collaboration, and ethical governance principles to create secure and reliable digital ecosystems.

REFERENCES

1. Edmund, E. and Enemosah, A., 2024. AI and machine learning in cybersecurity: Leveraging AI to predict, detect, and respond to threats more efficiently.
2. Olaoye, G., 2025. AI-Driven Intrusion Detection and Prevention Systems (IDPS) for Cloud Security. Available at SSRN 5129525.
3. Priyadharshini, S.L., Abbas, R., Arafat, Y., Batool, W., Abazi, U. and Altemimi, M.A., 2025. Cybersecurity in AI-Driven IT Environments: A Study on Vulnerabilities and Mitigation Strategies. Nanotechnology Perception, pp.1-19.
4. Konakanchi, S., 2025. Predictive Cyber-Resilience: AI-Powered Self-Defending Microservices for Zero-Downtime Security. Pioneer Research Journal of Computing Science, 2(2), pp.28-46.
5. Aiswarya, R.S., 2021. Cloud Infrastructure Security Using AI-Powered Threat Prediction and Mitigation. Journal of Techno Social, 13(1).
6. Edris, E.K.K., 2025. Utilisation of Artificial Intelligence and Cybersecurity Capabilities: A Symbiotic Relationship for Enhanced Security and Applicability. Electronics, 14(10), p.2057.
7. Savadatti, S., Kuldeep Dhariwal, S., Krishnamoorthy, S. and Delhibabu, R., 2024. An extensive classification of 5g network jamming attacks. Security and Communication Networks, 2024(1), p.2883082.
8. Mackay, B., 2024. AI Fundamentals Explained: From the early years of AI and machine learning to the future of AI. Brian Mackay.
9. Razavi, H., Ouaissa, M., Ouaissa, M., Nakouri, H. and Abdelgawad, A. eds., 2025. AI-Driven Cybersecurity: Revolutionizing Threat Detection and Defence Systems. CRC Press.
10. Algabri, H.K., 2025. AI and Cybersecurity-Innovations in Threat Detection and Prevention. Academic Guru Publishing House.
11. Al-Sawwa, J., 2025. Intelligence Systems. Strategic AI Integration in Business Intelligence, p.111.
12. Ali, T. and Kostakos, P. (2023). HuntGPT: Integrating Machine Learning-Based Anomaly Detection and Explainable AI with Large Language Models (LLMs). [online] arXiv.org. Available at: https://arxiv.org/abs/2309.16021?utm_source=chatgpt.com [Accessed 10 Nov. 2025].
13. Blessing Guembe, Misra, S., Azeta, A. and Lopez-Baldominos, I. (2025). Bibliometric analysis of artificial intelligence cyberattack detection models. Artificial Intelligence Review, 58(6). doi:https://doi.org/10.1007/s10462-025-11167-0.
14. editorialteam (2025). Threat Hunting with Machine Learning: How It Works - Apollo Technical LLC. [online] Apollo Technical LLC. Available at: https://www.apollotechnical.com/threat-hunting-with-machine-learning-how-it-works/?utm_source=chatgpt.com [Accessed 10 Nov. 2025].
15. Gupta, R. (2022). Artificial Intelligence in Cybersecurity: From Automated Threat Hunting to Self-Healing Networks. ESP Journal of Engineering & Technology Advancements (ESP-JETA), [online] 2(4), pp.92–104. Available at: https://www.espjeta.org/jeta-v2i4p117?utm_source=chatgpt.com [Accessed 10 Nov. 2025].
16. Merlano, C. (2024). Enhancing Cyber Security through Artificial Intelligence and Machine Learning: A Literature Review. Journal of Cyber Security, 6(1), pp.89–116. doi:https://doi.org/10.32604/jcs.2024.056164.
17. Ndayipfukamiye, T., Ding, J., Sarwatt, D.S., Gaston, P.A. and Ning, H. (2025). Adversarial Defense in Cybersecurity: A Systematic Review of GANs for Threat Detection and Mitigation. [online] arXiv.org. Available at: https://arxiv.org/abs/2509.20411?utm_source=chatgpt.com [Accessed 11 Nov. 2025].
18. Nwaodike (2025). AI-Powered Threat Hunting: Detecting Adversarial Machine Learning Attacks in Zero-Trust Environments. International Journal of Computer Applications Technology and Research. doi:https://doi.org/10.7753/ijcatr1112.1022.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411086|

19. Onih, V.A., Sevidzem, Y.S. and Adeniji, S. (2024). The Role of AI In Enhancing Threat Detection and Response in Cybersecurity Infrastructures. International journal of scientific and management research, 07(04), pp.64–96. doi:https://doi.org/10.37502/ijsmr.2024.7404.
20. Pillai, P. (2023). AI And ML In Cybersecurity | The Review Hive. [online] The Review Hive. Available at: https://thereviewhive.blog/ai-and-ml-in-cybersecurity/ [Accessed 10 Nov. 2025].
21. Rahmati, M. (2025). Towards Explainable and Lightweight AI for Real-Time Cyber Threat Hunting in Edge Networks. [online] arXiv.org. Available at: https://arxiv.org/abs/2504.16118?utm_source=chatgpt.com [Accessed 11 Nov. 2025].
22. reddit.com (2025). Reddit - The heart of the internet. [online] Reddit.com. Available at: https://www.reddit.com/r/redteamsec/comments/uyawuh/?utm_source=chatgpt.com [Accessed 10 Nov. 2025].
23. Reddy Kethireddy, R. (2022). AI-Driven Automated Threat Hunting with Predictive Analytics. JOURNAL OF RECENT TRENDS IN COMPUTER SCIENCE AND ENGINEERING, 10(1), pp.23–34. doi:https://doi.org/10.70589/jrtcse.2022.1.3.
24. Sewak, M., Sahay, S.K. and Rathore, H. (2022). Deep Reinforcement Learning for Cybersecurity Threat Detection and Protection: A Review. arXiv:2206.02733 [cs], [online] 1549, pp.51–72. doi:https://doi.org/10.1007/978-3-030-97532-6_4.
25. Shan, A. and Seunghwan Myeong (2024). Proactive Threat Hunting in Critical Infrastructure Protection through Hybrid Machine Learning Algorithm Application. Sensors, [online] 24(15), pp.4888–4888. doi:https://doi.org/10.3390/s24154888.
26. Thaqi, R., Krasniqi, B., Mazrekaj, A. and Rexha, B. (2024). Literature Review of Machine Learning and Threat Intelligence in Cloud Security. [online] doi:https://doi.org/10.20944/preprints202410.0512.v1.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details