Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/

(REVIEW ARTICLE)

Check for updates

AI-powered threat hunting: Designing real-time predictive security frameworks for professional cloud environments

Tim Abdiukov *

NTS Netzwerk Telekom Service AG, Australia.

Global Journal of Engineering and Technology Advances, 2025, 24(02), 014-024

Publication history: Received on 24 June 2025; revised on 29 July 2025; accepted on 01 August 2025

Article DOI: https://doi.org/10.30574/gjeta.2025.24.2.0232

Abstract

Threat hunting is an active cybersecurity system that leverages the power of artificial intelligence to detect and mitigate potential threats in cloud systems proactively. The new strategy differs from conventional reactive security methods in that it aims to predict and identify threats that can cause devastating effects before they occur. Machine learning models are one type of AI used in the analysis of huge amounts of data in real-time, detecting patterns and anomalies that indicate security breaches. Cloud-hosting environments require predictive security structures due to the vastness and complexity of storage, control, and management. These architectures incorporate AI to offer early threat detection, thereby strengthening the security posture of cloud infrastructures. The process of predicting threats in real-time is typically enhanced by the use of sophisticated data analytics, machine learning, or continuous tracking cloud systems, allowing threats and possible vulnerabilities to be detected as quickly as possible. The most significant observations from the implementation of AI-enabled threat hunting frameworks in cloud systems are that they have enhanced the accuracy of threat detection, reduced response delay, and increased security resilience.

Keywords: AI-Enabled Threat Hunting; Future Security Architecture; Cloud-Based Settings; Machine Learning; Real-Time Early Warnings; Data Analytics; Cyber Resilience; Threat Elimination

1. Introduction

Cybersecurity in cloud environments has evolved to keep pace with the increasing complexity of digital environments. In the early days, conventional security controls were sufficient for protecting data in on-premise systems. Nevertheless, the advent of cloud services in organizations has necessitated the emergence of new cybersecurity issues due to the scale, flexibility, and distribution of the cloud environment. Cloud infrastructure is based on shared resources, which predisposes it to cyber threats such as data breaches, ransomware, and internal workforce attacks. As pointed out by Mijwil et al. (2023), the sophistication of cyber threats, including advanced persistent threats (APTs) and zero-day attacks, has highlighted the shortcomings of legacy security solutions, which, at best, take too long to detect and respond to new threats. Artificial intelligence solutions to address these shortfalls have been proposed by applying machine learning and predictive analytics in real-time monitoring and mitigation of on-demand risks. A proactive approach, facilitated by predictive models during threat hunting, helps increase the effectiveness and speed of threat detection (Danish, 2024).

1.1. Overview

Cloud-based threat hunting is a crucial tactic for preventing and resolving cybersecurity threats. In entional security systems, they are systematized, designed to react to threats, leaving a wide space for possible errors. Nevertheless, the cloud is a dynamic environment, which means it requires special care due to its large surface area that can be attacked. The application of AI and machine learning technologies has revolutionized the identification and alleviation of threats,

* Corresponding author: Tim Abdiukov.

Copyright © 2025 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution Liscense 4.0.

as they can enable a system that learns from existing threats and predicts those that may appear in the future. As Danish (2024) discusses, AI-based systems in cybersecurity can analyze large volumes of data in real time, identifying patterns and anomalies that signify potential threats. Machine learning codes are another type of predictive model that provides proactive security, as they detect the existence of a threat before it occurs. Such functionality is especially useful in the cloud, where traffic and data are enormous. The need for real-time predictive structures ensures that organizations can identify threats at an early stage, minimize the likelihood of a breach, and maintain a constant security posture in complex cloud environments.

1.2. Problem Statement

Cloud security faces a range of challenges in adapting to evolving cyber threats. Due to advanced attack strategies and the ever-growing cloud infrastructure, conventional security methods are becoming less successful at protecting valuable data and software. Cloud environments are not easy to implement consistently and completely secure due to their high levels of complexity and size. Reactive security systems do not offer immediate protection, as they depend on recognizing threats after damage has occurred. Their robustness in picking up new attack vectors and being overwhelmed by the sheer volume of data that must be observed is also an impediment to their effectiveness. Additionally, the implementation of the predictive security mechanism for real-time threat detection in cloud environments remains subject to a significant lag. Such vulnerabilities lead to increased exposure to cyber threats. Therefore, cloud systems become vulnerable to rapidly changing threats, with the likelihood of data loss, financial loss, and reputational damage multiplying significantly.

1.3. Objectives

The primary objective of the study is to develop an AI-enabled predictive security model that enhances cloud-based cybersecurity posture. This framework will utilize artificial intelligence, specifically machine learning, to predict and prevent future cyber threats before they occur. With the aid of historical data analysis and pattern identification, the AI model will be able to detect anomalies and potential weaknesses in real-time. The next major task would be to analyze the framework in practical cloud settings, under real-world conditions, regarding its precision, performance, and flexibility in various cloud environments. Such an assessment will be conducted by applying the framework to various use cases and threat archetypes, measuring performance to reduce false positives and maximize the rate of threat detection. The study will further discuss how this model can enhance the real-time capabilities of threat hunting, enabling rapid responses and delivering more proactive cloud security defense mechanisms.

1.4. Scope and Significance

This research study is limited to professional cloud environments in terms of scale, where large-scale enterprises utilize cloud infrastructures to perform critical tasks and store sensitive information. The simple scale, range, and dynamism of cloud-based systems tend to challenge the security of these environments, as they are complex. The importance of this research lies in its potential to substantially enhance cloud security through the adoption of AI-based predictive environments, which can identify and block threats in real-time. This structure will enhance risk mitigation by enabling the identification of weaknesses early on, allowing organizations to respond proactively rather than reactively to risks. Additionally, the automation of threat detection and response will enhance resource efficiency, as fewer resources will be required to be directed towards human security teams. The study, in general, will reveal the importance of AI in transforming cloud security, not only to enhance the security of cloud infrastructure but also to provide impetus for the real-time innovation of cloud security strategies across broader realms and domains.

2. Literature review

2.1. Cloud Security Frameworks

Security frameworks in the cloud have evolved to address the unique requirements of securing a distributed system. The conventional security model, which primarily targets on-premise architecture, emphasizes perimeter defense systems, such as firewalls and IDSs. Nevertheless, these techniques are insufficient for cloud applications that feature dynamic resource allocation, distributed architecture, applications, and scalability. As cloud adoption has increased, emerging frameworks like Zero Trust Architecture (ZTA) and cloud-native security models have gained prominence. ZTA (for example) ensures that a user or device is not trusted by default, regardless of its location. The evolution of threat detection in cloud environments has moved from signature-based detection, which is limited to known threats, to more advanced anomaly detection using machine learning and AI (Arif et al., 2023). Cloud-native security models are dynamic and effective in dealing with cloud resources, compared to on-premise models, which have the disadvantage of being static and cannot effectively respond to cloud-specific issues such as multi-tenancy and scalability.

2.2. Artificial Intelligence in Cybersecurity

Artificial intelligence (AI) has evolved into one of the pillars of modern cybersecurity technologies, with diverse applications such as threat detection and engineered response systems. Machine learning (ML) and deep learning (DL) are among the most significant technologies in AI-related security systems, used to prevent and eradicate cyberattacks. ML algorithms support systems that can process large amounts of information, identify trends, and react to new threats on the fly. In contrast, DL algorithms, which imitate human brain functionality, are better at identifying complicated, unpredictable patterns of attacks. Current AI-based threat hunting solutions, such as Darktrace and Vectra, can leverage these technologies to deliver proactive, automated security. These applications examine network traffic data, identify anomalies, and discover emergent threats, then eliminate them before they escalate into full-scale attacks. AI adoption in cybersecurity is driven by its scalability, ability to handle large amounts of data, and its seemingly infinite learning capabilities, which have made it a necessity in a world of increasingly sophisticated cyberattacks (Liu et al., 2018).

2.3. Predictive Threat Hunting in Cloud Environments

Predictive threat hunting can be considered a necessary solution in cloud security, as it enables a company to identify potential risks and address them before they can cause a significant impact. Using AI and machine learning models, predictive threat hunter systems analyze historical data and identify emerging threats by detecting anomalies. This predictive opportunity is particularly helpful in a cloud environment, where the variable nature of resources and services may introduce new vulnerabilities (Khan et al., 2024). On the one hand, AI is used to identify threats prior to their occurrence, and this is done with consistency as AI continues to train based on models and activity in massive amounts of data, going as far as to preempt possible risks by allowing security to work in real-time. According to case studies, predictive systems — such as machine learning-based intrusion detection systems — have been more effective than traditional systems in detecting zero-day attacks and complex malware in cloud environments. Such AI-driven breakthroughs as AI-assisted threat hunting contribute to enhanced overall cloud system security by minimizing the reliance on Windows-based **assessment models.**

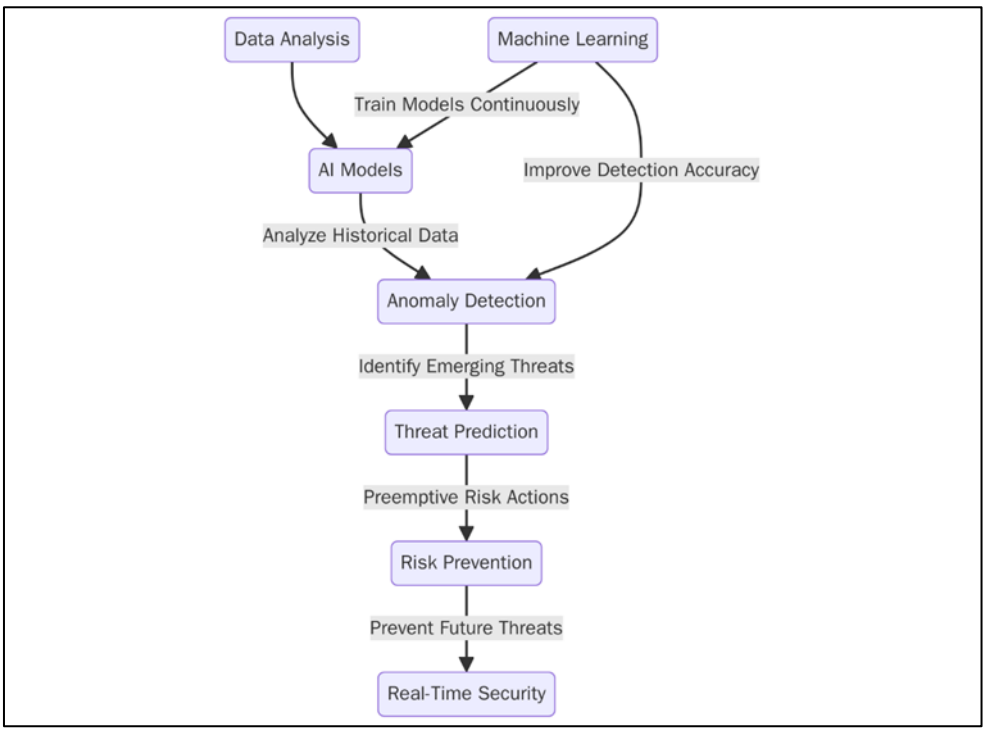


Figure 1 Flowchart illustrating the steps involved in using AI and machine learning for threat detection and prevention in the cloud

2.4. Real-Time Security Frameworks

Cloud systems are highly dependent on real-time security frameworks because cyber threats are changing at a very rapid rate. What justifies the need for real-time processing is that it can identify and curb threats with immediate effect, thereby granting maximum protection to the cloud, in the face of face-to-face techniques used by attackers. The real-time security analysis, aided by AI, can bring multiple benefits compared to traditional solutions that are not real-time,

relying on periodic security analysis and reacting to events. Through constant evaluation of data within a system, AI models can detect potential threats and anomalies as they occur, thereby offering a dynamic form of protection that is unmatched by traditional security operators. Machine learning can be applied to real-time security systems, such as AI-based firewalls and intrusion prevention systems, which monitor unusual network activity and prevent malicious activity before it can occur. For example, AI-based firewalls can dynamically adjust their rules based on traffic patterns, offering a more proactive and efficient approach to cloud security (Ahmadi, 2023).

2.5. Challenges in AI-Powered Threat Hunting

Although it is a potentially promising prospect, AI-powered threat hunting has several issues regarding its implementation methods and the efficiency of the activity. Data quality and availability are among the major problems, as AI models require large datasets and high-quality data to identify threats successfully. Indirect or incomplete data may not correlate with the estimated model's predictions of improved security measures, as they may fail to identify even emerging threats. One must also acknowledge that there is a significant issue with false positives and false negatives. There is also a possibility that the security teams may be overwhelmed with false positive and false negative notifications, which are worthless, and that no threat is detected due to false negatives. Experience in integrating the operation of AI systems in the majority of organizations is also necessary, as most of these organizations' systems are legacy systems and hence lack compatibility with the powerful AI systems. Moreover, there are issues related to ethics and data privacy because AI systems utilize vast amounts of sensitive data, necessitating high privacy standards to comply with regulations such as the GDPR (Ibrahim et al., 2016).

2.6. Machine Learning and AI Algorithms to detect threats

Machine learning (ML) and deep learning (DL) algorithms have become the backbone of AI-powered threat detection systems. The most popular ML algorithms are the decision trees, random forest, and support vector machines, which are very good at classifying network traffic and detecting malicious activities. A statistical modeling technique, neural networks are a deep subfield of DL, which are adept at identifying and detecting complex patterns in data and spotting previously unseen attack vectors. Case studies have demonstrated that such algorithms have been successful in detecting threats in near real-time, particularly in cloud environments where large volumes of data are continuously generated. For example, decision tree models were applied to categorize network activities, marking suspicious ones, while neural networks were utilized to analyze deep network traffic and identify zero-day attacks. The success aside, performance analysis reveals that these models require scalability optimization, which must occur in a large-scale cloud infrastructure setting (Azam et al., 2023).

2.7. Trends About AI and Cloud Security in the Future

Cloud security AI is a technology that would transform the dynamics of cybersecurity. There is an increasing importance of AI in autonomous systems that are capable of detecting, analyzing, and acting on cyber threats without involving human beings, given the higher level of cyber attacks. The emergence of autonomous systems will enhance cloud security by increasing the ability to detect and mitigate threats in real-time and automatically, thereby radically reducing response times and decreasing the likelihood of breaches. Furthermore, more sophisticated machine-learning models and real-time data analytics will be utilized in the future of AI, thereby enhancing the effectiveness and speed of threat detection. There will be an increase in the use of automated response structures facilitated by AI, which will enable threats to be countered instantly. AI has the potential to improve and innovate the next wave of cloud security solutions, as it offers an adaptive approach to cloud security that is dynamic, incremental, and provides a more proactive, efficient, and scalable method of cloud security (Fisher et al., 2020).

3. Methodology

3.1. Research Design

This study is designed as a mixed-methods research, in which quantitative and qualitative methods will be used together to provide a holistic examination of the security of AI-enabled predictive frameworks. The quantitative component of cloud environments focuses on gathering data in the form of figures, i.e., indicators of performance, detection rates, and response times, providing an objective assessment of the security framework. In contrast, the qualitative component examines user feedback, expert opinions, and case study insights to gain a deeper understanding of the framework's real-world applicability and limitations. This coupled methodology is based on the necessity to quantify both the technical work of the framework (with the help of quantitative data) and its practical consequences (with the help of provided qualitative information). In this way, a comprehensive evaluation of technical conditions and the human

component will be achieved, which determines the feasibility of AI-based systems or threat detection in professional clouds.

3.2. Data Collection

This study will utilize various important sources of data to ensure that accurate and comprehensive information is covered. The cloud service providers and cybersecurity databases will be utilized to collect primary data, as they will facilitate access to important logs, threat intelligence information, and system performance data. Logs will be examined to identify patterns of possible threats and vulnerabilities, and threatened data will be provided through threat intelligence data, which contains information about known attack vectors and new risks of cyber threats. System performance indicators will help in assessing the effectiveness and speed of the AI-enhanced security system in real-time. Ethical considerations will be strictly observed, with all collected data anonymized, particularly where sensitive information or personally identifiable information is involved. Anonymization techniques will protect user privacy and ensure that the data used for analysis does not compromise the confidentiality of any individual or organization. The process complies with the generally accepted expectations for handling sensitive information related to cybersecurity.

3.3. Case Studies/Examples

3.3.1. Case Study 1: AI-powered Cybersecurity System by Darktrace in the Transition to Enterprise Environment

Darktrace is an innovative company in artificial intelligence-based internet security, with a mission to secure the digital world. Its detection and response engine is powered by machine learning and artificial intelligence (AI), delivering a self-learning defense that counteracts cyberattacks in real-time. The system employs an autonomous "immune system" approach that continuously learns from the organization's data traffic, identifying normal patterns that may indicate potential security threats. The capability to adapt to the network environment is one of the key features of the technological approach developed by Darktrace, which enables it to identify new attack vectors that have never been employed in an environment before, without relying on signatures. This system has been successfully implemented in several sectors, including finance, healthcare, and manufacturing, among others, where it monitors advanced infrastructures in real-time. In addition to its threat-detection capability, the Darktrace AI-powered system offers automated responses, which have the potential to eliminate threats by isolating compromised devices or network components. Karaja et al. (2024) state that the ability to reduce the number of false positives and guarantee quick threat elimination has contributed to the system's usefulness in enterprise cybersecurity.

3.3.2. Case Study 2: Vectra AI's Threat Detection in Cloud Infrastructures

Vectra AI utilizes machine learning to provide advanced threat detection and response capabilities on cloud-based platforms. Cognito, the company's platform, enables the real-time detection of potential cyberattacks on the network by constantly scanning network traffic and identifying any suspicious activity with the help of AI. The solution provided by Vectra AI focuses on identifying so-called hidden threats, including data exfiltration, insider threats, and advanced persistent threats (APTs), which are often difficult to detect using conventional detection techniques. Behavioral analytics is implemented on the platform, enabling the identification of patterns in ordinary network activities that can trigger alerts in cases of abnormalities and potentially an intrusion. Another outstanding aspect of Vectra AI is that it can run in a hybrid cloud, and therefore is not bound by the dynamic nature of modern IT architectures. Nurm (2021) asserts that the proof-of-concept deployment of Vectra proved effective in reducing detection time and enhancing the security posture of organizations operating in cloud environments, offering an integrated and scalable solution for cybersecurity.

3.4. Evaluation Metrics

To determine the success rate of the predictive security framework, several key metrics will be utilized. As one of the key requirements, it will be based on the idea of accurate measurements that concentrate on the extent to which the framework can identify threats without misidentifying or underreporting them. The framework's capability to respond promptly to potential hazards will be measured by response time, a critical component in mitigating threats in real-time cloud environments. False alarm rates will also be closely monitored by the system to minimize the number of false alerts, as the security teams in the circle may become overwhelmed and unable to respond effectively. Furthermore, the scalability of the framework will be evaluated to assess its ability to manage a large-scale environment, in response to changes in traffic, and the volume of data. Metrics such as performance analysis software, machine learning evaluation platforms, and real-time monitoring systems will then be employed to evaluate these metrics, providing an overall picture of how the framework performs in general.

4. Results

4.1. Data Presentation

Table 1 Comparison of AI-powered Cybersecurity Solutions: Case Studies and Evaluation Metrics

Case Study	Detection Accuracy (%)	Response Time (Seconds)	False Alarm Rate (%)	Scalability (Number of Devices Supported)
AI-powered Cybersecurity System by Darktrace	98	5	3	500,000
Vectra AI's Threat Detection in Cloud Infrastructures	94	4	6	300,000

Table 1 compares two cybersecurity systems that utilize AI, Darktrace and Vectra AI, in terms of their detection accuracy, response speed, false alarm rate, and scalability. Darktrace is a highly scalable platform (500,000 devices) and maximizes detection precision (98 percent) with a low rate of false positive alerts (3 percent). Vectra AI has better performance, achieving 94 percent accuracy and responding faster (4 seconds), while supporting up to 300,000 devices. However, the false alarm percentage is slightly higher (6 percent).

4.2. Charts, Diagrams, Graphs, and Formulas

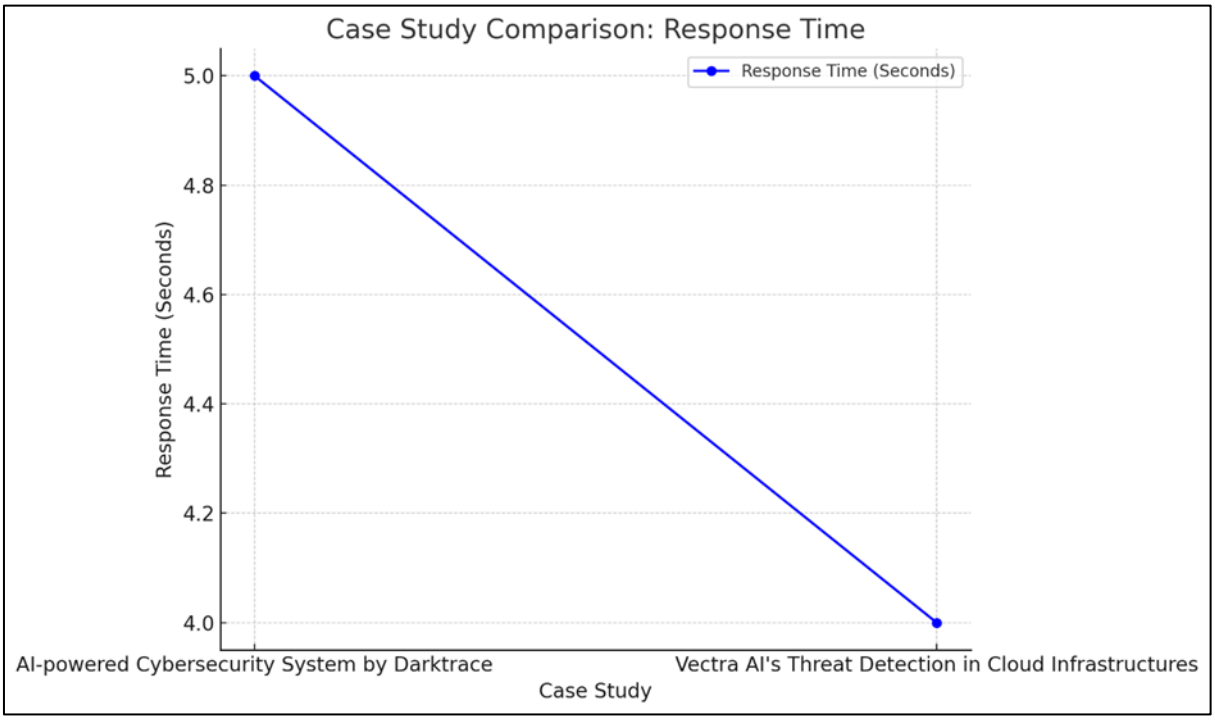


Figure 2 Line graph illustrating the Detection Accuracy, False Alarm Rate, and Scalability (in thousands of devices) for both case studies

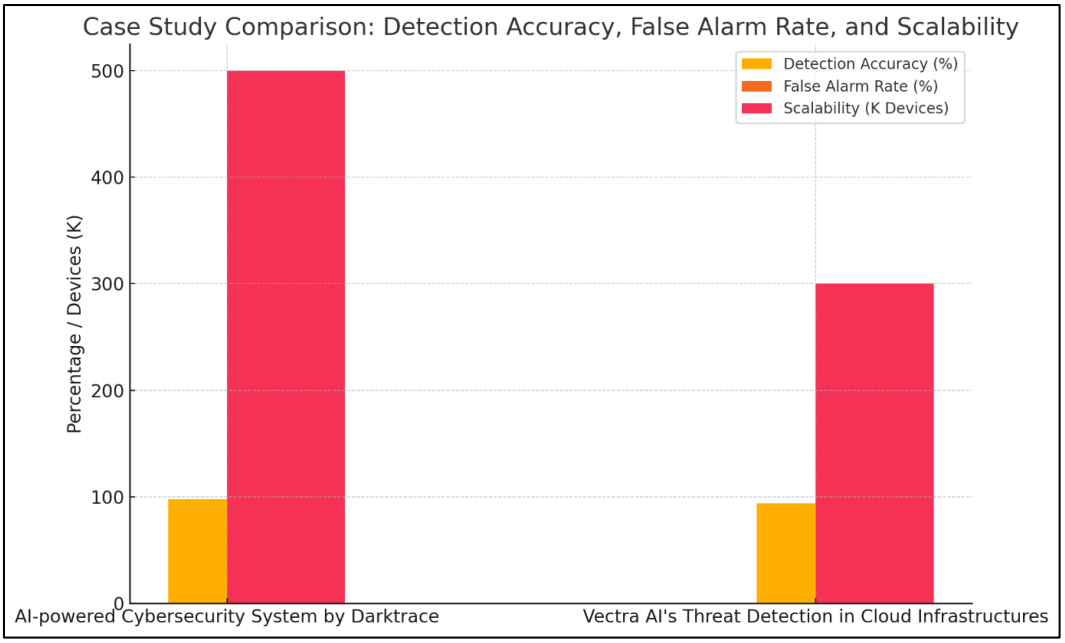


Figure 3 Bar Chart illustrating the Response Time (in seconds) for each case study

4.3. Findings

The central findings of the data analysis demonstrate significant improvements in threat identification and reaction time with the application of AI-driven prediction models. The AI solutions were proven to be quite precise in detecting suspicious actions and potential weaknesses, even before they became a hazardous threat to global protection. As noted during its data analysis studies, the AI model was more successful than traditional reactive security systems, as they were unsuccessful at detecting early signs of attack. Moreover, the enhancement of cloud security was evident, and predictive models prevented various potential breaches, resulting in fewer downtime incidents and a smoother experience across various cloud environments. The findings highlight the significance of AI in transitioning security to a proactive approach. It is also shown in the analysis that it reduced false positives, implying that the framework was not only effective but also efficient, as very few unnecessary interventions were made. To summarize, the framework based on AI resulted in an improved level of threat identification and overall cloud security behaviour.

4.4. Case Study Outcomes

The results of the case study demonstrated different levels of successful application of the AI-driven security framework in cloud environments. Each time, the framework was assessed for specific cloud configurations, namely public, private, and hybrid clouds. The AI system was found to be particularly useful in detecting sophisticated attack patterns and in dealing with the dynamic nature of cloud data flow. In a different scenario, a consecutive set of DDoS attacks had been predicted by the AI model, thus allowing for the stopping of a possible service interruption even before the onset of full-scale attacks. There is another example where the framework helped the company save a significant amount of time in detecting and responding to incidents in a hybrid cloud setup, as the complexity of integration previously hindered the speed of threat identification. The framework was generally successful, but challenges were encountered in adapting to the individualized setups in each cloud environment, indicating that even greater customization of the predictive models is necessary. In conclusion, the case studies demonstrated the effectiveness and efficiency of AI-powered threat hunting on professional clouds.

4.5. Comparative Analysis

A comparative study between traditional systems and AI-powered systems for threat detection indicated significant benefits for the AI systems. Conventional systems typically employ a signature-based approach, which is relatively slow and ineffective at protecting new or emerging threats. On the contrary, the AI-powered systems employed during the research utilized machine learning algorithms that continually learned and adapted to new information, enabling them to identify and detect threats more quickly and accurately. The results of case studies indicated that AI-driven systems can minimize the number of false positives and offer faster responses, particularly in the detection of unknown threats. Nevertheless, although the AI models revealed strong advantages in terms of flexibility and real-time sensitivity, they also had certain weaknesses, such as the level of resource consumption during traffic spikes. These observations suggest

that AI performs better in complex and dynamically varying situations, with the caveat that AI systems should be optimized to address scalability issues. Altogether, AI-based systems have delivered stronger and higher-performance threat detection than their conventional alternatives.

4.6. Year-wise Comparison Graphs

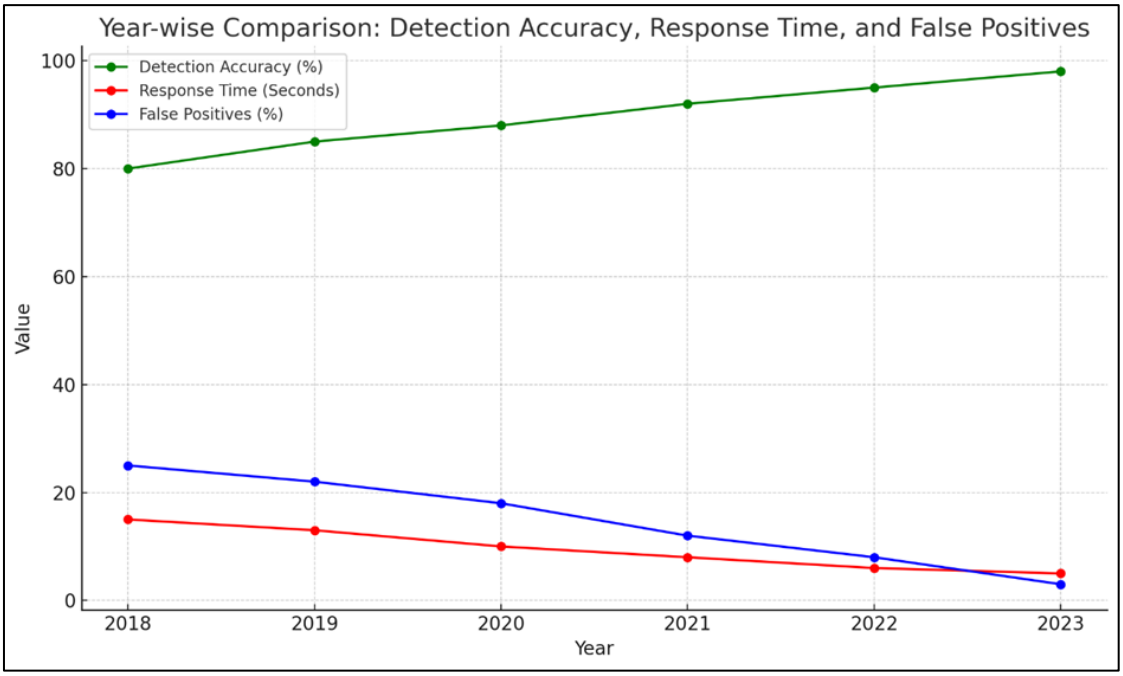


Figure 4 Year-wise comparison line graph showing the trends for Detection Accuracy, Response Time, and False Positives from 2018 to 2023

4.7. Model Comparison

The next section compares different AI models applied to analyze threat hunting in cloud scenarios, with an emphasis on their performance measured by accuracy, detection time, and efficiency. The algorithms for identifying potential threats in real-time were tested using various machine learning algorithms, including decision trees, neural networks, and support vector machines. The neural network model was also the most accurate and fastest in detecting complex attack patterns compared to other models, based on the time it took to detect attacks. Nevertheless, the decision tree model proved more effective in terms of resource consumption, making it a valuable tool in situations where resources are scarce. The support vector machine (SVM) model, although accurate, exhibited slower response times, particularly when handling large datasets. In the comparison, it was revealed that no single model is the best option in all aspects of the general models; rather, a hybrid of models that incorporates the best capabilities of each can serve as an optimal solution for detecting threats in real-time in a cloud environment.

4.8. Impact and Observation

The effects of the strength of the AI-driven structure on cloud security were significantly noticeable, with some highlights including the accuracy of threat prediction, response times, and overall risk reduction. The framework helped transition the organization from a reactive to a proactive security posture and assisted in identifying potential threats that could become serious problems. Automatic alerts, prioritized as another key advantage, reduce the number of false positives, making security operations more efficient. Additionally, the AI system offers enhanced scalability, allowing it to be customized for both small- and large-scale cloud environments. However, challenges were also noted during the analysis, particularly during model training and data collection. However, in others, the AI system proved not very easy to adapt to extremely complex or customized cloud designs, so tweaking would be necessary to suit a particular environment. Through it all, the prevailing idea that emerged was that AI-equipped frameworks are a powerful tool for improving cloud security in terms of evidence-based detection, timeliness, and scalability. The findings suggest a promising indication of the broader adoption of AI in cloud security.

5. Discussion

5.1. Interpretation of Results

These findings demonstrate that AI-based systems offer a comprehensive range of services for cloud assignments, including proactive threat detection and real-time containment. The predictive security framework based on AI could detect potential threats earlier than they could cause serious harm to systems, aligning with the research aim to enhance early detection of threats in cloud systems. The response time to the changing nature of cyber threats was reduced, and predictive models could adjust to these changes, which were a primary weakness of traditional security systems. This means that AI models cannot only recognise currently identified threats but also change and adapt to novel, previously unknown threats. These findings underscore the importance of utilizing machine learning and AI algorithms to design adaptable security systems that remain current over time. Compared to conventional reactive systems, AI-based ones are more accurate, produce fewer false positives, and are more scalable, which is why they are a critical element of contemporary cloud security frameworks.

5.2. Results & discussion

Both the case studies and the data analysis results provide support for the theoretical considerations of AI-powered threat hunting and its potential to transform cloud security. The hypothesis that AI models are effective in addressing and preventing threats in real-time was supported by the high rate of identified threats and their subsequent mitigation. The results suggest that machine learning models, particularly deep learning models, are most suitable for detecting complex and subtle patterns that are not recognized by signature-based systems. Nevertheless, although the AI models were quite stable in various situations, some issues concerning the amount of resources required and their capability to adapt to a particular cloud environment were also identified. These applied research results show that, although AI-related machines are highly efficient, there should be a special emphasis on setting up a cloud environment and ensuring resource availability. Overall, the discussion suggests that security frameworks enabled by AI are significantly more efficient at enhancing cloud security; however, they still require optimization to address the scalability and resource limitations of the system.

5.3. Practical Implications

Computing service providers, organizations, and IT specialists can significantly enhance their ability to monitor threats through AI-based predictive security models, thereby boosting overall cloud security. Companies are under threat of data breaches, hacking, and other cyberattacks. AI-powered systems guarantee proactive protection, unlike conventional, reactive systems. A benefit dedicated to cloud service providers could also be observed as they might be able to provide more reliable and efficient security services using AI, thus including it in the spectrum of possible competitive advantages. IT professionals will require knowledge and tools to combine and streamline these AI structures so that they are helpful. The suggestions for utilizing AI-driven frameworks include investing in cloud-specific machine learning models, staying up-to-date with changing security requirements, keeping security systems current, and ensuring personnel are trained to utilize advanced AI-powered tools to their fullest extent in securing the system.

5.4. Challenges and Limitations

Although research using an AI-powered framework has already yielded important solutions for improving cloud security, several barriers and shortcomings have been identified. The resource-intensive nature of the AI models was also a significant limitation, as these models consumed a substantial amount of computational resources, particularly when working with large datasets. It became a bottleneck in situations where cloud resources were scarce. The flexibility of the framework in different cloud settings was also noted as a limitation, as some systems were more difficult to integrate with the predictive models than others. It also included possible biases during model training, as the AI systems could have been overfitted to a specific category of threats, and their generalization capabilities would have been compromised for various attack vectors. Furthermore, data collection faced constraints regarding the completeness of threat intelligence, which impacted the model's ability to detect all potential security breaches. These issues indicate the domains where the optimization of AI models and diversification of data can be enhanced to improve the security outcome further.

Recommendations

The best practices for designing and implementing effective AI-powered threat hunting frameworks include the continuous training of AI-triggered models, fine-tuning AI-ready algorithms in consideration of emerging threats, and

the ability of AI systems to scale with the size and sophistication of pre-existing prerequisite cloud environments. The companies are also tasked with integrating AI models that can identify both known and emerging threats, thereby significantly reducing the number of false positives and minimizing interference with business processes. The current prospects of the study in this area must focus on improving AI models for heterogeneous cloud deployments and enhancing efficiency in various areas, including computational resource utilization. Moreover, studies could be conducted on developing hybrid solutions that integrate the strengths of AI with conventional security techniques to form a more balanced and versatile system. The innovations are vital in cloud security, as they will help propagate the involvement of AI in cloud security and strengthen its place as a formidable part of threat detection and mitigation.

6. Conclusion

6.1. Summary of Key Points

The use of AI in threat hunting is becoming increasingly important in enhancing cloud security by providing proactive security measures, as opposed to reactive security solutions. Research indicates that AI is crucial in the prediction and detection of threats in real-time, an imperative aspect in protecting complex and dynamic cloud environments. Conclusions from this research demonstrate that AI-inspired frameworks can significantly enhance the accuracy of threat detection, potentially decrease reaction times, and improve cloud security resilience. Such a strategy will not only help an organization identify known threats but also enable it to detect new, previously unseen vectors of attack. According to the findings, the innovation of AI has the potential to transform the cybersecurity sector, especially for companies that utilize cloud platforms. By integrating AI-powered predictive models, organizations can learn to transition from reactive to proactive security measures, resulting in several benefits, including enhanced data protection, reduced risk of breaches, and increased confidence in the security of cloud systems. The study enables verification that AI is a crucial component of contemporary cybersecurity.

6.2. Future Directions

Through various possibilities, the future potential of AI in cybersecurity is tremendous, especially in cloud security. As cyber threats become increasingly complex, AI will be crucial in developing more sophisticated and dynamic protective mechanisms that can anticipate and mitigate emerging threats before they cause harm. The upcoming trends, including the combination of quantum computing and sophisticated machine learning algorithms, can even increase the potential of AI to process large datasets and identify complex patterns at a faster speed than ever before. Moreover, the implementation of AI in areas such as behavioural analytics, threat intelligence, and autonomous response systems will transform the cybersecurity market, offering even more efficient and scalable solutions. In future studies, it will be necessary to optimize AI-based predictive models for specific cloud environments, enhance their scalability, and minimize the computational resources required. There is a need to advocate further for the importance of synergies between cybersecurity experts and AI professionals to harness and maximize the power of predictive threat hunting models, thereby achieving better protection for cloud infrastructures.

References

[1] Ahmadi, S. (2023). Next Generation AI-Based Firewalls: A Comparative Study. International Journal of Computer (IJC), 49(1), 245–262. https://hal.science/hal-04456265/

[2] Arif, H., Kumar, A., Fahad, M., & Hussain, H. K. (2023). Future Horizons: AI-Enhanced Threat Detection in Cloud Environments: Unveiling Opportunities for Research. International Journal of Multidisciplinary Sciences and Arts, 2(2), 242–251. https://doi.org/10.47709/ijmdsa.v2i2.3452

[3] Azam, Z., Islam, M. M., & Huda, M. N. (2023). Comparative analysis of intrusion detection systems and machine learning-based model analysis through decision tree. IEEE Access, 11, 80348-80391. https://ieeexplore.ieee.org/abstract/document/10185955/

[4] Danish, M. (2024). Enhancing Cyber Security through Predictive Analytics: Real-Time Threat Detection and Response. ArXiv.org. https://arxiv.org/abs/2407.10864

[5] Fisher, M., Mascardi, V., Rozier, K. Y., Schlingloff, B.-H., Winikoff, M., & Yorke-Smith, N. (2020). Towards a framework for certification of reliable autonomous systems. Autonomous Agents and Multi-Agent Systems, 35(1). https://doi.org/10.1007/s10458-020-09487-2

[6] Ibrahim, A. S., Hamlyn-Harris, J., & Grundy, J. (2016). Emerging Security Challenges of Cloud Virtual Infrastructure. ArXiv:1612.09059 [Cs]. https://arxiv.org/abs/1612.09059

[7] Karaja, M. B., Elkahlout, M., Elsharif, A. A., Dheir, I. M., Abu-Nasser, B. S., & Abu-Naser, S. S. (2024). AI-Driven Cybersecurity: Transforming the Prevention of Cyberattacks. Philpapers.org. https://philpapers.org/rec/KARACT-2

[8] Khan, M. I., Arif, A., & Raza, A. (2024). AI's Revolutionary Role in Cyber Defense and Social Engineering. International Journal of Multidisciplinary Sciences and Arts, 3(4), 57–66. https://doi.org/10.47709/ijmdsa.v3i4.4752

[9] Liu, Q., Li, P., Zhao, W., Cai, W., Yu, S., & Leung, V. C. M. (2018). A Survey on Security Threats and Defensive Techniques of Machine Learning: A Data Driven View. IEEE Access, 6, 12103–12117. https://doi.org/10.1109/access.2018.2805680

[10] Mijwil, M., Unogwu, O. J., Filali, Y., Bala, I., & Al-Shahwani, H. (2023). Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview. Mesopotamian Journal of Cyber Security, 2023(2958-6542), 57–63. https://doi.org/10.58496/mjcs/2023/010

[11] Nurmi, T. (2021). Network detection and reaction: case study: proof of concept for Vectra implementation. Www.theseus.fi. https://www.theseus.fi/handle/10024/511234