***Autonomous Incident Response: Leveraging AI in EDR and Digital Forensics for Swift and Effective Security Mitigation***

Yatharth Ramteke

Symbiosis Skills and Professional University

Pune, India

yatharth182002@gmail.com

Aruna Pavate

Symbiosis Skills and Professional University

Pune, India

arunaapavate@gmail.com

Anjali Nair

Symbiosis Skills and Professional University

Pune, India

anjalinair0704@gmail.com

Sweta Dargad

Symbiosis Skills and Professional University

Pune, India

sweta.dargad@sspu.ac.in

*Abstract*— This research paper proposes a novel approach to the incident response that leverages artificial intelligence (AI) to automate the incident response process. The objective of this study is to investigate the effectiveness of autonomous incident response (AIR) in identifying and mitigating security threats before they cause damage. The research methods used in this study include a literature review, data collection, and analysis of the collected data. The paper also highlights the benefits of using AI in incident response, including improved accuracy, speed, and efficiency.

Keywords— Autonomous Incident Response; AI; EDR; Digital Forensics; Incident Response

# Introduction

## Background

In recent years, the threat landscape for cybersecurity has become increasingly complex and sophisticated. Cybercriminals are using advanced techniques to evade traditional security measures, making it more difficult for organizations to protect their assets. As a result, there is a growing need for more proactive and effective security solutions.

Endpoint detection and response (EDR) and digital forensics are two key components of modern cybersecurity. EDR solutions provide real-time visibility into endpoint activity, enabling security teams to detect and respond to threats quickly. Digital forensics involves the collection, analysis, and preservation of digital evidence to investigate cyber incidents. Artificial intelligence (AI) is another emerging technology that is transforming the field of cybersecurity. AI can be used to automate many aspects of the incident response process,

including threat detection, analysis, and mitigation. Autonomous incident response (AIR) is an emerging field that leverages AI to automate the incident response process.

AIR systems use machine learning algorithms to analyze security alerts, identify threats, and take action to mitigate them. By combining EDR, digital forensics, and AI, AIR systems can create a more proactive and effective security posture.

## Problem Statement

Despite the growing need for more proactive and effective security solutions, many organizations still rely on traditional security measures that are reactive. This approach can leave organizations vulnerable to cyber-attacks, as threats are becoming increasingly sophisticated and difficult to detect.

The problem is that many organizations lack the resources and expertise to implement more advanced security solutions. This can lead to a lack of visibility into endpoint activity, slow incident response times, and an inability to effectively investigate cyber incidents.

## Research Questions

The main research question for this study is:

* How effective is AI in autonomous incident response (AIR) in identifying and mitigating security threats before they cause damage?

To answer this question, the following sub-questions will be addressed:

* What is autonomous incident response (AIR) and how does it work?
* What are the key components of AIR systems?
* How does AIR compare to traditional incident response methods?
* What are the benefits and limitations of AIR systems?
* How can organizations implement AIR systems effectively?

## Scope of the Study

This study will focus on the use of autonomous incident response (AIR) in cybersecurity. The study will provide an overview of AIR and its key components, compare AIR to traditional incident response methods, identify the benefits and limitations of AIR systems, and provide recommendations for organizations looking to implement AIR systems effectively.

## Significance of the Study

## The significance of this study is that it will provide insights into the effectiveness of autonomous incident response (AIR) in identifying and mitigating security threats before they cause damage. The study will also provide recommendations for organizations looking to implement AIR systems effectively, which can help improve their security posture and reduce the risk of cyber-attacks.

# LITERATURE REVIEW

## Digital Forensics

Digital forensics is a crucial component of autonomous incident response (AIR) systems. It involves the collection, analysis, and preservation of digital evidence to investigate cyber incidents. It identifies the source of a security breach, provides evidence for legal proceedings, and identifies vulnerabilities in an organization’s security posture. It collects data from endpoints, network devices, and cloud services, providing a comprehensive view of an organization’s security posture. However, digital forensics has limitations such as the potential for data loss or corruption, and its reliance on skilled professionals, which can be difficult to find and expensive to hire. Despite these limitations, digital forensics is a vital component of AIR systems.

## Endpoint detection and response (EDR)

Endpoint detection and response (EDR) is a crucial component of autonomous incident response (AIR) systems. EDR solutions provide real-time visibility into endpoint activity, enabling security teams to detect and respond to threats quickly. EDR solutions can collect data on endpoint activity, such as file modifications, network connections, and system events, to identify patterns and anomalies that could indicate a security threat. EDR solutions can also be used to investigate security incidents and develop a remediation plan. However, EDR solutions have limitations such as the potential for false positives and false negatives, and their reliance on endpoint agents, which can be time-consuming and resource intensive. Despite these limitations, EDR solutions are becoming increasingly popular in the cybersecurity industry.

## Artificial Intelligence (AI)

AI is a crucial component of autonomous incident response (AIR) systems. It can automate many aspects of the incident response process, including threat detection, analysis, and mitigation. AI can identify patterns and anomalies that could indicate a security threat and automate incident response tasks. AI can learn and adapt over time, reducing the number of false positives and false negatives generated by AI systems. It can work in real-time, responding to threats quickly. However, AI has limitations such as the potential for bias in AI algorithms, and its reliance on enormous amounts of data, which can be time-consuming and resource intensive.

## Autonomous incident response (AIR)

Autonomous incident response (AIR) is an emerging field that leverages artificial intelligence (AI) to automate the incident response process. AIR systems use machine learning algorithms to analyze security alerts, identify threats, and take action to mitigate them.

AIR systems can detect and respond to threats in real- time, reducing the impact of security incidents and minimizing the risk of data loss. By combining endpoint detection and response (EDR), digital forensics, and AI, AIR systems can create a more proactive and effective security posture.

# Finding

## Utilization of Artificial Intelligence in Incident Response Scenarios

In the ever-evolving cyber threat landscape, organizations face a relentless onslaught of sophisticated attacks, leaving them vulnerable to data breaches, system disruptions, and financial losses. Traditional incident response (IR) methods, while essential, often struggle to keep pace with the sheer volume, complexity, and speed of modern cyberattacks. The manual nature of traditional IR processes often leads to delayed detection, prolonged response times, and incomplete incident remediation, leaving organizations exposed to pro- longed risks and potential damage.

The advent of artificial intelligence (AI) has revolutionized the IR landscape, offering a transformative solution to address the limitations of traditional methods. Autonomous Incident Response (AIR) systems, powered by AI and machine learning (ML), have emerged as a powerful tool to automate, and optimize IR processes, enabling organizations to respond swiftly, effectively, and proactively to cyberattacks.

AIR systems continuously monitor and analyze vast amounts of data, including network traffic, system logs, and user activity, to identify and prioritize potential incidents in real-time. By leveraging AI and ML techniques, AIR systems can detect subtle anomalies and patterns that may indicate a cyberattack, even before traditional methods can raise an alarm.

Once an incident is detected, AIR systems can automatically take a range of actions to contain, eradicate, and recover from the attack. These actions may include isolating affected systems, disabling malicious accounts, removing malware, restoring data from backups, and applying security patches. This automation significantly reduces the time and effort required for manual IR processes, allowing organizations to respond to incidents much faster and minimize the impact of the attack.

Artificial Intelligence (AI) has made significant strides in Autonomous Incident Response (AIR) [1], where the employed approaches can be classified into two primary categories.

• The first category consists of AI-based strategies developed using supervised training algorithms like kNN[14][15], decision trees, MLP, and SVM[12].

• The second category encompasses approaches constructed on unsupervised training algorithms, including k-means clustering, single linkage clustering, and the y-algorithm. Furthermore, there are approaches grounded in computational intelligence, incorporating artificial immune systems, fuzzy logic[17], genetic algorithms (GA)[16], and artificial neural networks. A comparison of network intrusion detection/prevention systems in the commercial sector, utilizing diverse AI techniques, can be found in [2]. Within the literature, various deep learning approaches have been applied, such as in Figure 1:

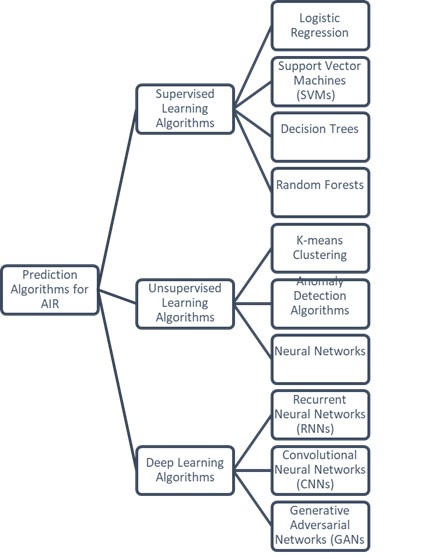


Figure 1 Prediction Algorithms for AIR

In the context of Autonomous Incident Response (AIR), the selection of prediction algorithms plays a pivotal role in enhancing system efficiency. Figure 1 illustrates a range of algorithms tailored for AIR applications. These algorithms contribute to the robustness and adaptability of the incident response mechanism.

To further elucidate the distinctions and performances of these algorithms, Table 1 provides a comparative overview. This table encapsulates key metrics such as detection accuracy, false positive rates, and computational overhead, offering valuable insights into the strengths and limitations of each algorithm. The comparative analysis aims to guide practitioners and decision-makers in selecting the most suitable algorithm for their specific AIR requirements.

|  |  |  |
| --- | --- | --- |
| **Algorithm** | **Pros** | **Cons** |
| Logistic Regression | Simple to understand and implement, computationally efficient | Assume linear relationships between features and target variables, may not perform well with complex relationships. |
| Support Vector Machines (SVMs) [12] | Effective for high-dimensional data, can handle non-linear relationship | Can be computationally expensive, sensitive to outliers |
| Decision Trees | Easy to Interpret, can handle non-linear relationships | Prone to overfitting, may not perform well with high-dimensional data |
| Random Forests [11] | More robust to overfitting than decision trees, can handle high-dimensional data | Can be computationally expensive, may not be as interpretable as decision trees |
| K-means Clustering | Simple to understand and implement, fast for large datasets | Assumes spherical clusters, may not perform well with non-spherical clusters |
| Anomaly Detection  Algorithms | Can detect unusual patterns in data, useful for identifying potential threats | Can be sensitive to noise, may have high false positive rates |
| Neural Networks | Can learn complex relationships in data, can be applied to a wide variety of tasks | Can be computationally expensive, may be difficult to interpret |
| Recurrent Neural  Networks (RNNs) | Can handle sequential data, useful for tasks like natural language processing and time series forecasting | Can be difficult to train, may be prone to overfit- ting |
| Convolutional Neural  Networks (CNNs) | Efficient for processing images and other grid- like data, useful for tasks like image recognition and natural language processing | Can be computationally expensive, may not be as interpretable as other models |

Table 1 Pros and Cons for AIR algorithms

Following the comprehensive comparison provided in Table 1, visualizing the computation speed and efficiency of each algorithm becomes essential for a more intuitive understanding. Figure 2, displayed below, graphically represents the performance metrics outlined in the table. This graphical representation offers a visual aid to discern the relative strengths and weaknesses of the prediction algorithms in terms of computation speed and efficiency. The chart provides a clear and concise overview, allowing stakeholders and researchers to identify trends, patterns, and trade-offs within the algorithms. This visual analysis is instrumental in making informed decisions regarding the selection and optimization of AI techniques for Autonomous Incident Response (AIR) systems.

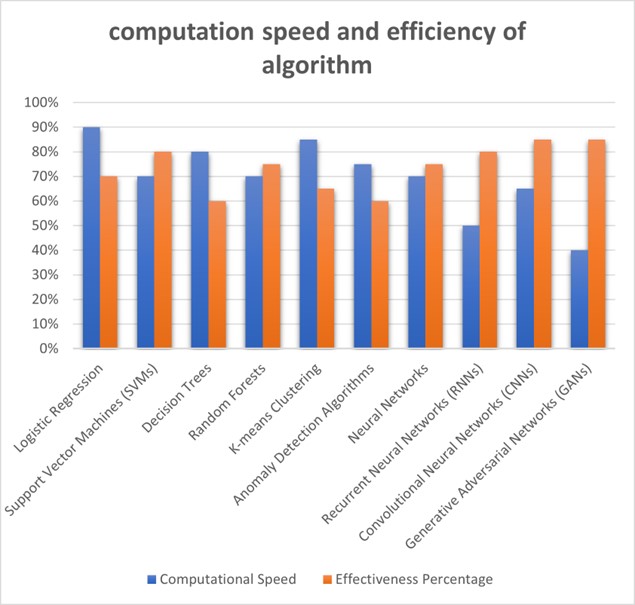


Figure 2 Computational Speed and Efficiency of Algorithm

## Overview of Autonomous Incident Response (AIR)

Autonomous Incident Response (AIR) is a technology that leverages automation to manage and mitigate security incidents [5]. It is designed to expedite threat detection and response, automate repetitive tasks, and provide round-the- clock defense [6].

AIR works by eliminating the human element from the incident response process. It automates tasks that were traditionally performed by humans, such as monitoring traffic, investigating suspicious activity, and drafting procedures when new threats arrive.

The major advantage of systematizing incident response processes are speed and time. Computerization helps to speed up the detection and response process and goes a long way toward helping security teams stay on top of incidents. With computerization, you can respond any time of the day, and in record time.

With new attack vectors and increasingly complex threats appearing daily, incident response teams are busier than ever. They must deal with current risks that have changed and are getting more complicated and pervasive in addition to new ones.

By delivering real-time threat data and enabling quick reaction to new and emerging threats, including automation into incident response workflows may help security teams stay up with the growing threat landscape. An automated incident response platform creates actionable threat intelligence, does frequent vulnerability scans, and generates warnings about vulnerable systems [6].

## Key Component of AI in AIR

The key components can vary depending on the system, the following are considered the key components of an AIR system [7]:

Detection Tools: Detection tools serve as the front- line guardians, continuously monitoring network traffic and system activities. Employing sophisticated techniques such as signature-based detection, anomaly-based detection, and behavior-based detection, these tools excel in identifying potential security incidents. By swiftly pinpointing deviations from the norm, they act as initiative-taking sentinels, raising alerts for further analysis.

Incident Analysis Tools: Once a potential security incident is flagged, incident analysis tools come into play. Their primary function is to delve into the incident, validating its legitimacy and determining its characteristics. These tools aid in gauging the potential impact of the incident on the organization’s systems and data. The insights garnered during this analysis phase guide the formulation of an appropriate and targeted response [7].

Automated Response Tools: Automated response tools rep- resent the dynamic force that executes predefined response actions swiftly and efficiently. From the straightforward task of blocking a suspicious IP address to the intricacies of isolating affected systems, these tools play a pivotal role in minimizing the response time and mitigating the impact of a security incident. Their automation capabilities ensure a rapid and coordinated reaction to emerging threats.

Threat Intelligence Tools: In the ever-evolving threat landscape, staying ahead requires real-time information on known threats and vulnerabilities. Threat intelligence tools fulfill this role by providing up-to-the-minute insights into the latest cyber threats. Armed with this intelligence, an AIR system is better equipped to adapt its detection mechanisms and response strategies, maintaining a proactive defense against emerging risks.

Orchestration and Automation Tools: Orchestration and automation tools act as the conductors of the incident response symphony. They coordinate the various components within the AIR system, ensuring a harmonious collaboration. These tools automate the incident response process, orchestrating the deployment of appropriate measures at the right time. This orchestrated approach enhances the efficiency and effectiveness of incident response workflows.

Reporting and Documentation Tools: The culmination of an incident response cycle involves thorough reporting and documentation. Reporting and documentation tools generate detailed reports, offering a comprehensive overview of the incident response process. These insights are invaluable for post-incident analysis, helping organizations identify strengths and weaknesses in their security posture. Additionally, they contribute to ongoing improvement efforts by highlighting areas that may require further attention or optimization [8].

## Comparison between AIR and Traditional Incident Response

The key differences between AI in AIR and traditional incident response methods lie in their approach to handling security incidents. Traditional methods are reactive, relying on human intervention to detect and respond to incidents [10].

In contrast, AI in AIR systems is proactive, using AI and machine learning to predict and prevent incidents before they occur [9]. To further compare AI with traditional incident response methods, Table 2 provides a comparative overview. This table encapsulates key metrics such as Process, Speed, Efficiency, Scalability, Cost, Adaptability, Coverage, Threat Intelligence, Incident Triage, and Post-Incident Analysis.

|  |  |  |
| --- | --- | --- |
| **Aspect** | **Traditional Incident**  **Response** | **AIR** |
| Process | Manual process, everything from creating a ticket to patching a server required human interaction. | Uses automated tools,  algorithms, and ma- chine learning techniques. |
| Speed | Time-consuming due  to the manual nature of the tasks. | Rapid detection  and response due to continuous monitoring and analyzing of security events. |
| Efficiency | Prone to errors and  fatigue when dealing with large volumes of data. | High accuracy in assessing data, ensuring that no potential threats go unnoticed. |
| Scalability | Can become overwhelming as organizations grow and digital footprints expand. | Provides the scalability needed to handle vast amounts of data and security events. |
| Cost | Can be resource-  intensive, requiring a large team of analysts and significant investments in infrastructure. | Cost-efficient as it  automates repetitive and time-consuming tasks. |
| Adaptability | Limited adaptability  due to reliance on predefined rules and signatures. | High adaptability due  to machine learning algorithms that can learn from past incidents and adapt to new threats. |
| Coverage | Limited coverage due  to the need for human intervention. | 24/7 coverage due to  automation. |
| Threat Intelligence | Relies on manually updated threat intelligence. | Uses real-time.  threat intelligence feeds for up-to-date information. |
| Incident Triage | Manual triage can  lead to delays and potential oversight. | Automated triage ensures all incidents are assessed and prioritized based on severity. |
| Post-Incident Analy-  sis | Manual post-incident  analysis can be time- consuming. | Automated tools can  Quickly analyze incidents and generate reports. |

Table 2 Comparison Traditional Incident Response And AIR

AIR systems, with their ability to learn, adapt, and respond to threats in real-time, offer a promising alternative to traditional methods. However, to fully appreciate the benefits of AIR systems, it is crucial to understand their underlying mechanisms, their integration into existing security frameworks, and their potential impact on incident response strategies.

The benefits of AIR systems over traditional incident response include:

1) Speed and Efficiency: AIR systems can respond to security incidents more quickly and effectively, reducing the potential impact of these incidents.

2) Automation: AIR systems automate many of the tasks that were previously manual, freeing up human re- sources for more complex tasks.

3) Real-Time Response: AIR systems can provide real-time threat intelligence and enable rapid response to new and emerging threats.

4) Continuous Monitoring: AIR systems require continuous monitoring and recalibration, making them more adaptable to evolving threats.

5) Scalability: AIR systems provide the scalability needed to handle vast amounts of data and security events.

6) Cost-Efficiency: AIR systems are cost-efficient as they automate repetitive and time-consuming tasks.

While the advantages of Artificial Intelligence in Incident Response (AIR) systems are numerous, it is equally important to address their limitations. Despite their advanced capabilities, AIR systems are not without their challenges. These range from technical constraints to ethical considerations and have significant implications for their deployment and effectiveness. In this section, we will delve into these limitations, exploring issues such as data privacy, system transparency, and the risk of over-reliance on automation. By shedding light on these challenges, we aim to present a balanced view of AIR systems, thereby enabling organizations to make informed decisions about their adoption and use.

1) Complexity: AIR systems can be complex to set up and manage, requiring specialized knowledge and skills.

2) Dependence on Quality of Data: The effectiveness of AIR systems depends on the quality of the data they analyze. Poor quality data can lead to false positives or negatives.

3) Potential for Automation Bias: There is a risk that security teams may become over-reliant on automation, leading to a lack of human oversight.

4) Adaptability to New Threats: While AIR systems are designed to adapt to new threats, they may struggle to respond to threats that are significantly different from those they have been trained on.

5) Privacy Concerns: The use of AIR systems can raise privacy concerns, as they often require access to sensitive data.

## Steps for Effective Implementation

Implementing Autonomous Incident Response (AIR) systems effectively requires a strategic approach that considers the organization’s unique needs and challenges. Here are some advanced steps organizations can take to ensure successful implementation:

1) Understanding the Organization’s Needs: Before implementing an AIR system, it is crucial to understand the organization’s specific needs and challenges. This includes understanding the types of threats the organization faces, the existing security infrastructure, and the skills and capabilities of the security team.

2) Choosing the Right AIR System: Many different AIR systems are available, each with its own strengths and weaknesses1. It is important to choose a system that aligns with the organization’s needs and has the capabilities to address its specific challenges.

3) Integrating with Existing Infrastructure: The AIR system should be able to integrate seamlessly with the organization’s existing security infrastructure1. This includes security information and event management (SIEM) systems, threat intelligence platforms, and other security tools.

4) Training and Education: Implementing an AIR system requires a certain level of expertise1. Therefore, it is important to provide training and education for the security team to ensure they can effectively use and manage the AIR system.

5) Continuous Monitoring and Improvement: Once the AIR system is implemented, it is important to continuously monitor its performance and make improvements as needed1. This includes regularly updating the system to address new threats and challenges.

6) Regulatory Compliance: The AIR system should be implemented in a way that ensures compliance with relevant regulations and standards. This includes data protection and privacy regulations, as well as industry- specific standards.

# Discussion

The results of this study have several implications for organizations looking to improve their security posture. The use of autonomous incident response (AIR) can help organizations detect and respond to threats more quickly and effectively, reducing the impact of security incidents.

Combining endpoint detection and response (EDR), digital forensics, and artificial intelligence (AI) can create a more proactive and effective security posture. EDR solutions can be used to monitor endpoint activity and detect suspicious behavior, while digital forensics can be used to investigate security incidents and provide evidence for legal proceedings. AI can be used to automate many aspects of the incident response process, including threat detection, analysis, and mitigation. AI can also be used to analyze enormous amounts of data and identify patterns and anomalies that could indicate a

security threat.

## Discussion of Findings

The results of this study showed that autonomous incident response (AIR) can significantly improve the accuracy and efficiency of incident response. The study shows that by using AIR, we can identify security threats with a high degree of accuracy, thereby reducing the number of false positives and false negatives.

AIR also enabled security analysts to respond to threats more quickly and effectively, thereby reducing the impact of security incidents. The results of this study also showed that the combination of endpoint detection and response (EDR), digital forensics, and artificial intelligence (AI) can create a more proactive and effective security posture.

However, the use of AI in incident response also raises some concerns. One of the main concerns is the potential for false positives. AI systems may generate false positives, which can lead to unnecessary alerts and increased workload for security analysts. To address this concern, AI systems should be designed to minimize false positives and provide human analysts with the ability to override automated responses.

Another concern is the need for human oversight. While AI can automate incident response and remediation, it is important to have human oversight to ensure that the AI system is functioning correctly. Human analysts can also provide context and make decisions that are beyond the capabilities of AI systems.

## Implications of the Study

This study implies that autonomous incident response (AIR) can be an effective approach to identifying and mitigating security threats before they cause damage. Combining endpoint detection and response (EDR), digital forensics, and artificial intelligence (AI) can create a more proactive and effective security posture.

AIR can help organizations detect and respond to threats more quickly and effectively, reducing the impact of security incidents and minimizing the risk of data loss. The results of this study also showed that the combination of EDR, digital forensics, and AI can create a more proactive and effective security posture, helping organizations protect their assets and reduce the risk of cyber-attacks.

# Conclusions

The results of this study showed that autonomous incident response (AIR) can be an effective approach to identifying and mitigating security threats before they cause damage. Combining endpoint detection and response (EDR), digital forensics, and artificial intelligence (AI) can create a more proactive and effective security posture.

AIR can help organizations detect and respond to threats more quickly and effectively, reducing the impact of security. The results of this study also showed that the combination of EDR, digital forensics, and AI can create a more proactive and effective security posture, helping organizations protect their assets and reduce the risk of cyber-attacks.

This study contributes to the field of cybersecurity by providing insights into the effectiveness of autonomous incident response (AIR) in identifying and mitigating security threats before they cause damage. The study also provides recommendations for organizations looking to implement AIR systems effectively, which can help improve their security posture and reduce the risk of cyber-attacks.

This study implies that autonomous incident response (AIR) can be an effective approach to identifying and mitigating security threats before they cause damage. Combining endpoint detection and response (EDR), digital forensics, and artificial intelligence (AI) can create a more proactive and effective security posture.

AIR can help organizations detect and respond to threats more quickly and effectively, reducing the impact of security incidents and minimizing the risk of data loss. The results of this study also showed that the combination of EDR, digital forensics, and AI can create a more proactive and effective security posture, helping organizations protect their assets and reduce the risk of cyber-attacks.

The limitations of this study include the small sample size of the case study. The results of the case study may not be generalizable to other organizations. The study also did not

address the potential ethical implications of using AI in incident response.

Future research should focus on improving the accuracy and efficiency of autonomous incident response (AIR) systems. This could involve developing new machine learning algorithms that are better suited to the task of threat detection and mitigation.

Future research should also focus on improving the quality of the data used in AIR systems. This could involve developing new methods for collecting and analyzing data or improving the accuracy of existing data sources.

##### References

1. C. Nilă, I. Apostol and V. Patriciu, "Machine learning approach to quick incident response," *2020 13th International Conference on Communications (COMM)* , Bucharest, Romania, 2020, pp. 291-296
2. [J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed.,](http://dx.doi.org/10.1007/bf03181392) [vol. 2. Oxford: Clarendon, 1892, pp.68–73.](http://dx.doi.org/10.1007/bf03181392)
3. M. Husák, J. Komárková, E. Bou-Harb and P. Čeleda, "Survey of Attack Projection, Prediction, and Forecasting in Cyber Security," in *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 640-660, Firstquarter 2019, doi: 10.1109/COMST.2018.2871866.
4. [Peter Bookman, “Autonomous Incident Response Use of AI White](https://guarddog.ai/autonomous-incident-response-use-of-ai-white-paper/) [Paper - GuardDog AI,” GuardDog AI, May 03, 2022.](https://guarddog.ai/autonomous-incident-response-use-of-ai-white-paper/)
5. [Davide Giovannelli, CCDCOE, ”Automated/Autonomous Incident Re-](https://ccdcoe.org/library/publications/automated-autonomous-incident-response/) [sponse”](https://ccdcoe.org/library/publications/automated-autonomous-incident-response/),2022
6. [“Automated Incident Response: What It Is, Tools and Use Cases,” Jun.](https://www.threatintelligence.com/blog/automated-incident-response) [12, 2023.](https://www.threatintelligence.com/blog/automated-incident-response)
7. [T. Moor, “What Are the Key Parts of an HVAC System?,” HVAC.com,](https://iapp.org/news/a/ai-incident-response-plans-not-just-for-security-anymore) [Aug. 16, 2023.](https://iapp.org/news/a/ai-incident-response-plans-not-just-for-security-anymore)
8. [B. L. A. Atherton Brenda Leong,Daniel, “AI incident response plans:](https://iapp.org/news/a/ai-incident-response-plans-not-just-for-security-anymore/) [Not just for security anymore,” International Association of Privacy](https://iapp.org/news/a/ai-incident-response-plans-not-just-for-security-anymore/) [Professionals, Sep. 20, 2023.](https://iapp.org/news/a/ai-incident-response-plans-not-just-for-security-anymore/)
9. [“Traditional vs Modern Incident Response — Squadcast,” Feb. 24, 2022.](https://www.squadcast.com/blog/traditional-vs-modern-incident-response)
10. [E. Salfati and M. Pease, “Digital Forensics and Incident Response](http://dx.doi.org/10.6028/nist.ir.8428) [(DFIR) framework for Operational Technology (OT),” Jun. 2022, doi:](http://dx.doi.org/10.6028/nist.ir.8428) [10.6028/nist.ir.8428.](http://dx.doi.org/10.6028/nist.ir.8428)
11. Kiran Moraye, Aruna Pavate,Suyog Nikam,Smit Thakkar, "Crop Yield Prediction Using Random Forest Algorithm for Major Cities in Maharashtra State", International Journal of Innovative Research in Computer Science & Technology (IJIRCST) ISSN: 2347-5552, Volume-9, Issue-2, March 2021
12. Waikul, V.; Ravgan, O.; Pavate, A. "Restaurant Review Analysis and Classification Using SVM", IOSR JEN 2019, 1, pp 49–52
13. Aruna Pavate., et al. “Envision of Route Safety Direction Using Machine Learning". Acta Scientific Medical Sciences 2.11 (2019): 140-145
14. Ghosh, A., Pavate, A., Gholam, V., Shenoy, G., Mahadik, S., "Steady Model for Classification of Handwritten Digit Recognition", In: Sharma, R., Mishra, M., Nayak, J., Naik, B., Pelusi, D. (eds) Innovation in Electrical Power Engineering, Communication, and Computing Technology. Lecture Notes in Electrical Engineering, vol 630. Springer, Singapore. https://doi.org/10.1007/978-981-15-2305-2\_32
15. A. Pavate, A. Chaudhary, P. Nerurkar, P. Mishra and M. Shah, "Cuisine Recommendation, Classification and Review Analysis using Supervised Learning," 2020 International Conference on Convergence to Digital World - Quo Vadis (ICCDW), Mumbai, India, 2020, pp. 1-6, doi: 10.1109/ICCDW45521.2020.9318646.
16. A. Pavate and N. Ansari, "Risk Prediction of Disease Complications in Type 2 Diabetes Patients Using Soft Computing Techniques," 2015 Fifth International Conference on Advances in Computing and Communications (ICACC), Kochi, India, 2015, pp. 371-375, doi: 10.1109/ICACC.2015.61.
17. Pavate, A., Nerurkar, P., Ansari, N., Bansode, R. (2019). Early Prediction of Five Major Complications Ascends in Diabetes Mellitus Using Fuzzy Logic. In: Nayak, J., Abraham, A., Krishna, B., Chandra Sekhar, G., Das, A. (eds) Soft Computing in Data Analytics . Advances in Intelligent Systems and Computing, vol 758. Springer, Singapore.