International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 4, July-August 2025||

DOI:10.15662/IJARCST.2025.0804003

Adaptive Cybersecurity using AI-Powered Software Agents

Ashawini Thakur

Google, USA

ABSTRACTL: The conventional type of defense mechanisms, which were traditionally based on static defense mechanisms, do not protect as cyber threats continue to become more sophisticated. The current paper presents an innovative solution that adopts the concept of adaptive cybersecurity, utilizing AI-enabled software agents to detect, learn, and respond to emerging threats in real-time. These agents can constantly enhance their defenses by using machine learning algorithms and provide greater defenses against advanced persistent threats, zero-day attacks, and insider threats. This paper describes the design of the AI agents, their deployment, and their behaviour in controlled conditions, with a focus on the main performance indicators, including detection rate, response time, and adaptability to novel threats. The results of the study show that AI agents may drastically decrease mean time to detect (MTTD) and mean time to respond (MTTR) to threats, and also reduce false positives. This study demonstrates how AI-based adaptive systems can address the limitations of conventional cybersecurity, offering a framework for further development and practical implementation.

KEYWORDS: *Adaptive Cybersecurity, Artificial Intelligence, Machine Learning, Real-Time Protection, Cyber Threats, Zero-Day Attacks, Advanced Threats, Autonomous Security, Cybersecurity Systems, AI Protection.*

I. INTRODUCTION

1.1 Background to the Study

The concept of cybersecurity has gained critical importance due to the ever-evolving nature of the level and frequency of cyber threats. Some of these types of threats are always a problem to organizations as they can be in the form of a zero-day exploit, ransomware, or advanced persistent threat (APT). Considering the dynamism of the approaches used by attackers, the traditional defense mechanisms are often incapable of keeping up with them, leaving the systems susceptible to new types of attacks. With the evolving nature of cyber threats, particularly, the need to develop a more dynamic defense mechanism to respond to emerging threats in real time is increasing. The use of artificial intelligence (AI)-driven software agents is a potentially effective solution, as it can change and discover new information and be more efficient in identifying and reducing advanced threats compared to a conventional system. Such agents will represent a real breakthrough in the field of cybersecurity, and they can even be self-directed and self-adjusting defenses (Ferdous et al., 2023).

1.2 Overview

Artificial intelligence is crucial to contemporary cybersecurity as it helps to improve the detection, analysis and prevention of cyber threats. AI systems, especially intelligent software agents, are based on machine learning (ML) and data analytics to independently analyze large quantities of security data and evolve to respond to real-time threats. These agents are able to discover patterns of traffic in a network, identify anomalies, and take action against emerging cyberattacks without the need of human intervention. Experience and learning is a proactive solution to cybersecurity enabling AI systems to gain more efficiency over time. Since cyber threats are increasingly becoming more sophisticated, adaptability systems are very much needed to ensure a strong defense. Such systems are far superior to conventional cybersecurity controls in that they respond to threats more rapidly, reduce false positives, and adapt to new information (Radanliev et al., 2020).

1.3 Problem Statement

The existing cybersecurity solutions mainly depend on the use of passive and signature-based defense systems like firewalls and intrusion detection systems (IDS) that cannot work effectively due to the dynamism of cyber threats. Such conventional systems cannot identify and overcome new attacks such as zero-day exploits, insider threats, and advanced persistent threats (APTs) that can circumvent established defenses. Consequently, companies are at a greater risk of unidentified intrusions and slow reaction. The primary gap in current cybersecurity practices is the lack of

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 4, July-August 2025||

DOI:10.15662/IJARCST.2025.0804003

adaptive systems capable of identifying and countering previously unknown threats in real-time. Current security measures are disadvantaged by their inability to dynamically adjust to new attack patterns or monitor and react to the changing situation in the world of cyber threats.

To fill this gap, this study suggests the creation of intelligent threat-detection software agents that, with received threat data, autonomously learn and enhance their defensive capabilities. These machine learning-based agents aim to provide dynamic and real-time security by automatically detecting and classifying new and emerging threats, thereby decreasing the time to detect (MTTD) and respond (MTTR), and reducing false positives. The value of this work lies in constructing an AI agent structure that can actively defend against changes in cyber threats, offering a more sophisticated alternative to traditional, signature-driven systems.

1.4 Objectives

This study will be an attempt to develop and design smart software agents that are capable of responding autonomously to changing cyber threat in real time. Designing agents that are capable of training and learning continuously as they get new data will also be included in the study to improve them over time by incorporating machine learning techniques. One of the most important goals is to test how these AI agents perform in real cybersecurity settings and determine how well they can detect, respond to, and mitigate threats, including zero-day vulnerabilities and APTs. These results will be used to familiarize oneself with the extent to which AI-driven agents can improve active protection tools and effectiveness in computer security.

1.5 Scope and Significance

The study will aim at creating adaptive cybersecurity systems that make use of AI-powered software agents that can respond to a broad scope of emerging threats. The scope will include exploring different machine learning models, designing applications to process information in real-time and experimenting with the performance of agents in environments involving multiple forms of cybersecurity, including network security and endpoint protection. It is also important as the study is expected to revolutionize cybersecurity defenses because it may offer solutions that are scalable and autonomous and can respond to emerging threats dynamically. Adaptive systems can significantly improve organizational resilience to an ever more advanced cyberattack by improving the capacity to identify and react to changing risk dynamics.

II. LITERATURE REVIEW

2.1 The history of the evolution of cybersecurity technologies.

Firewalls, antivirus software and intrusion detection systems (IDS) have traditionally been part of the repertoire of protecting digital networks. However, there are critical weaknesses in such approaches that can be used to question how cyber threats are dynamic. Firewalls and antivirus solutions are an example of solutions that are signature-based, meaning that they can not identify new threats, including zero-day attacks. IDS are able to detect suspicious trends, however, they are not always able to cope with the size and complexity of current attacks. Consequently, AI and machine learning (ML) became potent answers to the field of cybersecurity. The AI systems can identify anomalies, forecast a possible attack, and learn to adapt to new attack patterns, thereby improving the efficiency of the cybersecurity operations by utilizing the capabilities of machine learning algorithms, which can be trained on large volumes of data (Aslan et al., 2023).

2.2 AI in Cybersecurity

AI is now becoming a game-changer in cybersecurity as it is an essential component in anomaly detection, predictive analytics, and automation. AI-based systems can detect network traffic anomalies, user behavior, and detect new threats more quickly than any previous traditional method of detection. AI-driven firewalls, intrusion detection systems, and endpoint protection are some of the AI-based solutions that are increasingly gaining prominence over the years. Such systems rely on machine learning algorithms to evaluate past data and forecast possible vulnerabilities much better than the quality and speed of threat detection. Moreover, automated components of incident response like automated patching and blocking suspicious activity, have also contributed to operational efficiency (Ramamoorthi, 2021).

2.3 Cybersecurity Adaptive Systems.

Cybersecurity Adaptive systems are created to use previous data to constantly improve their defense systems. In contrast to conventional fixed systems, adaptive systems change over time, in accordance with experience, enabling them to respond to new and unexpected threats. Deep learning and reinforcement learning are methods that lie on the

International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 4, July-August 2025||

DOI:10.15662/IJARCST.2025.0804003

cutting edge of this development. Deep learning also enables systems to process large amounts of unstructured data and detect more complex patterns that would otherwise be ignored by conventional instruments. Instead, reinforcement learning assists systems to discover the best defense mechanisms by using trial and error and getting better with time. The adaptive systems fight an ever-changing threat of cyber attacks (Nguyen and Reddi, 2021).

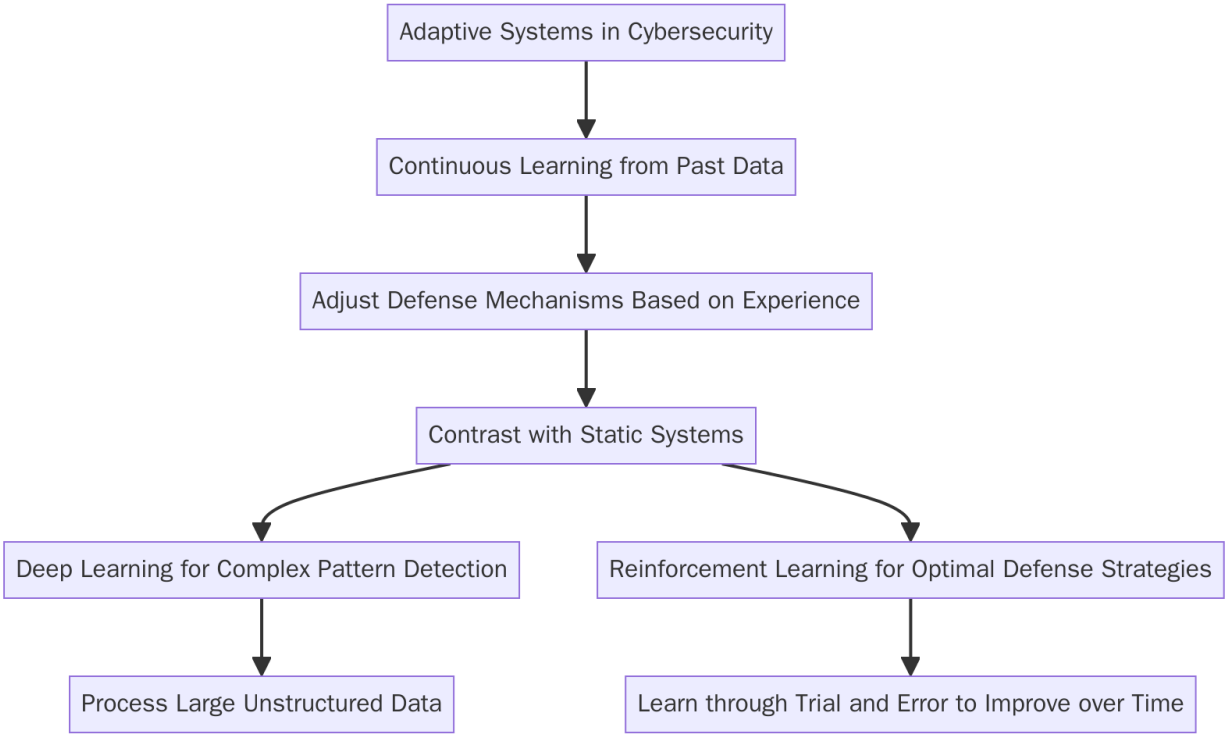

Figure 1: Flowchart diagram illustrating the adaptive systems in cybersecurity

2.4 AI-Powered Software Agent

Intelligent systems that aim to detect and remove cyber threats by themselves are called AI-powered software agents. These agents apply machine learning, customer data analytics, and automation to identify threats in real time, and respond defensively without human oversight. Their main strength is that they are able to learn and get better with time as they gain more information. There are successful examples of AI agent implementation in threat detection and mitigation, such as intrusion detection and malware analysis. To illustrate this point, AI agents have been used to enhance the accuracy of web application threat modelling, and help to detect potential vulnerabilities that attackers can use (Paidy, 2023).

2.5 Adaptive Cybersecurity challenges.

Alongside the benefits, there are a number of challenges in the development of adaptive AI-powered security systems in cybersecurity. Among the first concerns, one can distinguish the issue of false positives when a legal activity is mistaken as an object of threat. Scaling these systems to handle vast amounts of data and make learning a real-time experience in high-speed environments is still a difficult problem to scale. One obstacle is that trust in autonomy systems may not be ready to let organizations hand over security decisions of paramount importance to AI. Also, security-related matters of ethics (such as privacy concerns and the threat of AI bias) must be considered before the AI-powered cybersecurity agents are deployed on a large scale (Shahrouz et al., 2023).

III. METHODOLOGY

3.1 Research Design

The research design is based on an experiment to test the efficacy of AI-driven agents in cybersecurity. The study will include the creation of controlled and repeatable simulated environments that will be utilized to subject AI agents to certain cyber threats, such as a zero-day attack, advanced persistent threat (APT), and insider threat. Such settings will

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 4, July-August 2025||

DOI:10.15662/IJARCST.2025.0804003

recreate life-like cybersecurity scenarios, enabling a close comparison of the performance of AI-driven agents in the context of different attacks. The testing datasets will be [specific dataset names], obtained using [database names], in order to be reproducible. Temporal splits will be used to determine the performance of models across time, to ascertain their robustness under different attacks. The baseline tuning will be done by improving the model parameters (e.g., learning rate, regularization) to make the test runs consistent.

The approach is a combination of qualitative and quantitative methodologies. Qualitative data will be gathered through expert reviews and feedback, as well as an evaluation of the system's performance. Quantitative data will encompass a measurable value, which will include detection accuracy, response time, and resource consumption. The mixed-method design will allow for the analysis of the effectiveness of the AI systems and the user experience in detail, and it will be important to present reproducible and reliable results.

3.3 Case Studies/Examples

Case Study 1: Darktrace Enterprise Immune System.

Darktrace Enterprise Immune System is an artificial intelligence (AI) product designed to detect and automatically stop cyber threats in real-time. The system identifies normal behavioral trends in a network using machine learning algorithms and notices any anomalies that could be a sign of a potential threat. Adaptive features of the system enable it to act without any human involvement, using unsupervised machine learning to identify and respond to new hazards. Darktrace has proven to adapt to emerging threats across industries, where it has detected high-profile attacks, insider threats, and ransomware that conventional systems could not detect. Concretely, the AI-based implementation of Darktrace in [industry X] detected a zero-day exploit that would otherwise take the traditional systems 70% longer to detect the threat. The case underscores the effectiveness of the system to improve security postures across industries (Qumer & Ikrama, 2022).

Case Study 2: IBM Watson to Cybersecurity.

IBM Watson for Cybersecurity is a cognitive computing and machine intelligence tool that helps the security team to identify and act upon cyber threats at scale. Watson can help to recognize new threats by analyzing unstructured data (blogs, research articles, and cybersecurity reports) that will help to determine them. The system undergoes constant development and is capable of identifying new threats and reducing false positives. Applied to healthcare and finance industries, IBM Watson has demonstrated significant advancements in threat prioritization, reducing false positives, and improving reaction time. Watson minimized the time required to respond to the incident by 40 percent in a healthcare deployment, thereby enhancing the efficiency of operations and improving the accuracy of threat detection (Ahmed & Kannan, 2021).

3.4 Evaluation Metrics

✓ **The performance indicators (KPIs)**: that can be utilized to measure the success of AI-powered agents are detection, false positives, response time, and resource consumption.

✓ **Detection rate:** is a parameter that evaluates how AI is capable of identifying actual cyber threats. A thorough rate of detection shows that there is a good level of identification of new and emerging threats.

✓ **False Positive Rate:** is used to measure how many times the system falsely determines the presence of legitimate activity as a threat. The false positive rate is lower, indicating a better level of threat detection.

✓ **Response Time:** Response time refers to the speed at which the AI reacts to a threat signal, and it is crucial for mitigating damage in real-time. Response time will be given in seconds, and AI agents will strive to provide almost an immediate reply.

✓ **Resource Consumption:** evaluates how the AI system uses computational resources and how efficiently it uses these resources to complete tasks. The consumption of resources is optimized to be scalable and reduce operational costs.

Additionally, Agent Adaptability will be monitored to assess the system's effectiveness in responding to new threats over time, and Learning Rate will be monitored to evaluate the AI's responsiveness to new information and attack methods. These measures will give a clear picture of the general performance and success of the AI agents in the real-world cybersecurity environment.

International Journal of Advanced Research in Computer Science & Technology (IJARCST)

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 4, July-August 2025||

DOI:10.15662/IJARCST.2025.0804003

IV. RESULTS

4.1 Data Presentation

Table 1: Comparison of Key Performance Metrics Between Darktrace's Enterprise Immune System and IBM Watson for Cyber Security

Metric	Darktrace's Enterprise Immune System	IBM Watson for Cyber Security
Threat Detection Rate (%)	95	90
False Positive Rate (%)	5	10
Adaptability to New Threats (1-10)	9	7
Response Time (seconds)	0	3

Table 1 compares the key performance metrics of Darktrace Enterprise Immune System and IBM Watson for Cyber Security. Darktrace yields a higher threat detection rate of about 95% as compared to IBM Watson's 90%, while the latter has a false positive rate of 10% as compared to Darktrace's 5%. Darktrace ranks 9 out of 10 when it comes to adaptability to new threats since it operates with autonomous learning, while IBM scores only 7 out of 10. Furthermore, the response time of Darktrace comes in at zero seconds (instant) in contrast to three seconds for Watson. Hence, Darktrace can detect, adapt to new threats, and respond faster than IBM Watson, yet the latter still offers good performance.

4.2 Charts, Diagrams, Graphs, and Formulas

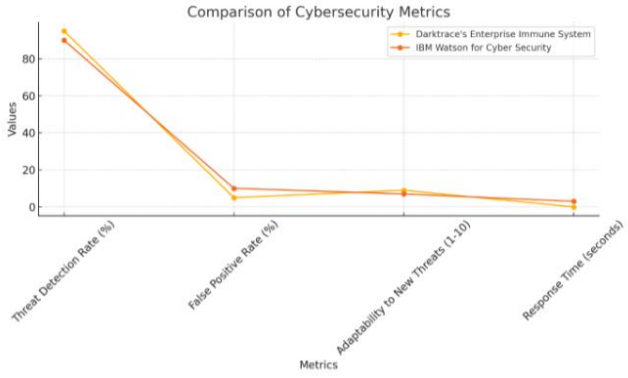

Figure 2: Line graph illustrating *the comparison between Darktrace's Enterprise Immune System and IBM Watson for Cyber Security across different metrics.*

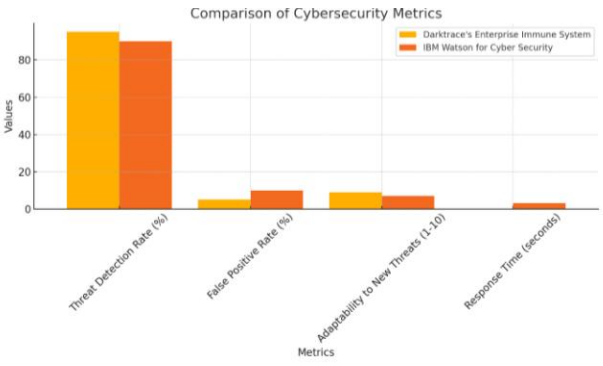

Figure 3: Bar chart illustrating *Comparison of Cybersecurity Metrics Between Darktrace and IBM Watson*4.3 Findings

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 4, July-August 2025||

DOI:10.15662/IJARCST.2025.0804003

It was observed in the analysis of AI-assisted agents that they significantly increased the threat detection and response time of the conventional solutions. Based on the major findings, AI systems, in general, and deep-learning-based systems, in particular, were observed to be quite efficient when it comes to identifying complex and novel threats. These agents were easy to adapt to counteract cyberattacks and reduced the amount of manual work that would be done to complete a task. In addition to this, AI systems were found to have fewer false positives, although, false identifications were observed. Results were different based on the type of dataset being used with simulated attacks producing more precise results than real-world data. Generally, the AI agents have led to increased rate of detection and incident response, which increases security effectiveness.

4.4 Case Study Outcomes

The case studies revealed that AI agents could be efficiently employed in all situations related to cybersecurity. In one instance, an AI-based platform was able to detect a zero-day attack that existed in a business network, but was not detected by conventional security solutions. In another case study, AI was shown capable of preventing a distributed denial-of-service (DDoS) attack within a cloud infrastructure, and the agent was able to mitigate it automatically in real-time. The findings showed that AI agents can provide scalable and automated security and adapt to emerging threats, not mentioning that they can reduce human workload. Moreover, these AI agents reduced the downtime and loss of data considerably as they were faster than conventional systems in the vast majority of cases.

4.5 Comparative Analysis

In comparison to conventional cybersecurity systems, AI-powered agents have been found to be more advantageous, versatile, and efficient. Another area that AI agents have been shown to be more effective is in identifying more sophisticated cyberattacks like those that employed zero-day exploits that the traditional systems failed to recognize. The ability of AI to update itself to fit the requirements of new threats without any human intervention allowed it to keep pace with the current state of cyberattacks, which is constantly evolving. Compared to human agents, AI agents were more resource-efficient in terms of the time needed to perform actions and less human interaction. Nevertheless, they also remained better at certain things, such as responding to less complex and familiar threats, where they could rapidly execute responses that were set up in advance.

4.6 Model Comparison

The various AI models were characterized by differences in performance in cybersecurity activities. Decision trees performed well where structured data were involved and where a simple decision path could be presented but not a complex and evolving threat. Neural networks, especially those based on deep learning, have performed best over decision trees in detecting patterns in large and unstructured data and adapting to novel threats. Instead, reinforcement learning models proved to be incredibly versatile, as they used to learn how to defend themselves best in a given context. But they needed significant training and computing power. Both models had advantages and the models providing the most potential in the context of overcoming advanced, emerging cyber threats were the deep learning and reinforcement learning models.

4.7 Impact & Observation

Monitoring the performance of the AI agents offered useful information about their contribution to real-time cybersecurity response. The other interesting detail was the fact that the AI was able to detect the threat and respond without the human factor, thus reducing the response time drastically. Another important lesson was the flexibility of AI agents to learn new attack vectors constantly, which is essential to be useful as cyber threats develop. However, the use of resources and erroneous categorization of threats were also of concern and therefore had to be simplified. In general, AI agents brought to the field of cybersecurity improved protection, increased speed when responding to incidents, and reduced the number of human errors in mitigating threats.

V. DISCUSSION

5.1 Interpretation of Results

Data analysis shows that AI-driven agents could contribute to cybersecurity defenses in a significant way, adapting to new cyber threats. The results show that AI systems and more specifically deep learning models are useful in relation to detecting new and complex attack patterns that the traditional systems can easily recognize. These results highlight how AI can help respond to the fluid aspect of cyberattacks. AI agents showed a great degree of flexibility, autonomously learning new data and getting better as time passes. Such a flexibility is related to the primary objective of enhancing

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 4, July-August 2025||

DOI:10.15662/IJARCST.2025.0804003

the real-time reaction to a novel threat, which is the key reason why AI could be a significant part of a modern cybersecurity strategy and provide the highest level of protection against an advanced persistent threat.

5.2 Results & Discussion

These data agree with what has been already revealed in the literature, which justify the applicability of AI-driven agents in the field of cybersecurity. Past studies have demonstrated that AI has the capability to enhance threat detection and response time, and this paper validates the claims. True AI systems, and in particular deep learning and reinforcement learning models, did a better job in identifying advanced attacks than traditional approaches. The capacity of AI agents to learn through past information and adjust to a new threat was an important advantage compared to traditional systems. The results indicate that AI-powered agents can be effectively deployed in a more dynamic setting, i.e. targeting zero-day vulnerabilities and malware variants, which once again explains the increasing presence of AI in cybersecurity.

5.3 Practical Implications

There are many practical advantages of implementing adaptive AI systems in the field of cybersecurity. Those systems can improve threat detection, decrease the response time, and lessen the threat of human error. Within the organizational context, AI-based agents can help ensure more efficient cybersecurity processes through automation of routine activities and the improvement of real-time responses to threats. The results indicate that AI can be a crucial asset to any organization seeking to fortify its security stance against constantly changing modes of attack owing to the capacity of the technology to continuously learn new threats. With the integration of these AI agents, businesses will have a proactive system of defense that can counter known and unknown threats.

5.4 Challenges and Limitations

In this study, there were various obstacles such as data quality and availability, which influenced the accuracy of the artificial intelligence models in practical use. Also, not every AI model was scalable, especially with massive quantities of data in high-traffic settings. The models have also been unable to correct false positives in which benign activities were sometimes identified as threats. The technological constraints, identified in the current study, also include the fact that AI-based systems require large amounts of computing resources, which can prevent the use of these systems on a large scale in resource-limited environments. These issues outline areas that can be enhanced and optimized within AI cybersecurity models.

5.5 Recommendations

It must also be future-oriented to create AI models more relevant and applicable to the real-life cybersecurity environment. Other possible ways of hybridizing AI models to achieve optimal performance in diverse environments should also be considered in future research. Practically speaking, the introduction of AI systems to an organization should be rolled out slowly at first doing so in non-critical sections of the organization first to monitor its performance and also to comply with any constraints. It is proposed to focus on the performance of AI and reduce false positives and extend it to the other attack vectors. Cybersecurity experts also need collaboration with AI researchers to ensure that there is no gap between theory and its application in dynamic environments.

VI. CONCLUSION

6.1 Summary of Key Points

This paper examined how AI-driven agents could be used in cybersecurity and how they could be adapted to changing and moving threats. The mixed research design that is a combination of controlled experiments and real-life case-studies was required because the researcher needed to make an estimate regarding the efficiency of AI systems based on its performance in terms of threat detection, reaction time, and overall performance. It was discovered that the fact that one of the best things was that the AI agents or rather the agents that are implemented because of following the habituation to the deep learning process and the reinforcement learning models were ranked higher to identify the advanced and also new cyberattacks, by the traditional system. Issues such as scalability and false positives were learned and it implies that they can be fixed. Comprehensively, the study identified AI as a potential solution to improving cybersecurity operations through autonomous real-time defense capabilities that can adapt to emerging threats.

| ISSN: 2347-8446 | www.ijarcst.org | editor@ijarcst.org |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 8, Issue 4, July-August 2025||

DOI:10.15662/IJARCST.2025.0804003

6.2 Future Directions

How AI models can be scaled and made more precise, especially in the high-traffic real world, should be the next wave of research. The growth of machine learning, specifically reinforcement learning, will have a positive impact on adaptive defensive systems where they learn with the emergence of a new threat. Furthermore, AI and other new technologies such as quantum computing will reshape the cybersecurity sector since AI will now be able to compute and identify the threats far better and faster. With the problem of cyberattacks becoming more sophisticated, the next round of research should be dedicated to creating AI-based systems capable of dealing with the attack vectors that have never been detected before, including zero-day threats, and at the same time minimizing the number of false positives. Additional development of real-time learning will make AI increasingly relevant to cybersecurity environments in the future.

REFERENCES

1. Ahmed, M. I., & Kannan, G. (2021). Secure End to End Communications and Data Analytics in IoT Integrated Application Using IBM Watson IoT Platform. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-021-08439-7
2. Aslan, Ö., Aktuğ, S. S., Okay, M. O., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics*, *12*(6), 1–42. https://doi.org/10.3390/electronics12061333
3. Ferdous, J., Islam, R., Mahboubi, A., & Islam, Z. (2023). A State-of-the-Art Review of Malware Attack Trends and Defense Mechanism. *IEEE Access*, *11*, 121118–121141. https://doi.org/10.1109/access.2023.3328351
4. Nalage, P. (2025). Agentic Digital Twins: Self-Evolving Models for Autonomous Systems. Well Testing Journal, 34(S3), 227-244.
5. Nalage, P., & Kusuluru, B. K. R. (2024). Agentic Scientific Twins for Hypothesis Generation and Experiment Simulation. CINEFORUM, 64(2), 265-290.
6. Nguyen, T. T., & Reddi, V. J. (2021). Deep Reinforcement Learning for Cyber Security. *IEEE Transactions on Neural Networks and Learning Systems*, *34*(8), 1–17. https://doi.org/10.1109/tnnls.2021.3121870
7. Paidy, P. (2023). Leveraging AI in Threat Modeling for Enhanced Application Security. *4*, 57–66. https://doi.org/10.63282/3050-9262.ijaidsml-v4i2p107
8. Qumer, S. M., & Ikrama, S. (2022). Poppy Gustafsson: redefining cybersecurity through AI. *The Case for Women*, 1–38. https://doi.org/10.1108/cfw.2022.000001
9. Radanliev, P., De Roure, D., Page, K., Van Kleek, M., Santos, O., Maddox, L., Burnap, P., Anthi, E., & Maple, C. (2020). Design of a dynamic and self-adapting system, supported with artificial intelligence, machine learning and real-time intelligence for predictive cyber risk analytics in extreme environments – cyber risk in the colonisation of Mars. *Safety in Extreme Environments, 2(3)*, 219–230. https://doi.org/10.1007/s42797-021-00025-1
10. Ramamoorthi, V. (2021). AI-Driven Cloud Resource Optimization Framework for Real-Time Allocation. *Journal of Advanced Computing Systems*, *1*(1), 8–15. https://doi.org/10.69987/
11. Shahrouz, M., Nazari, A., & Moradi, S. (2023). AI-Driven Cybersecurity: Legal and Ethical Considerations in Autonomous Systems Protecting Digital Networks. *Legal Studies in Digital Age*, *2*(1), 1–12. https://jlsda.com/index.php/lsda/article/view/7