Exploring the Applications of AIML in Cybersecurity

Kirti Arora, Shivani Thakur

Department of Computer Applications

Chandigarh School of Business, Jhanjeri

Chandigarh Group of Colleges, Jhanjeri, Mohali, India

kirtiarora2912@gmail.com
shivani.j1866@cgc.ac.in

Abstract- **The rapidly evolving field of cybersecurity encounters new threats and challenges as technology develops. The application of machine learning and artificial intelligence has become a viable way to improve cybersecurity measures in recent years. AIML is being used more and more in cybersecurity applications to enhance threat identification, mitigation, and response. The purpose of this research paper is to investigate the application of AIML in cybersecurity and how it can improve intrusion detection, network security, security analytics, and incident response. The study will look at particular applications of AIML in cybersecurity and show how it is superior to more conventional approaches. We will focus on using AI and ML to detect anomalies in network traffic, recognize and address cyber threats, improve security operations, and respond to incidents. We can better understand how AI and ML might be used to strengthen cybersecurity protocols and shield individuals, businesses, and countries from potential cyberattacks by looking into these areas. The results of this study will help to clarify the advantages and restrictions of AIML in cybersecurity and offer guidance for further investigation into the topic.**

Keywords:- Cybersecurity, Artificial Intelligence, and Machine Learning.

I. Introduction

The growing field of cybersecurity faces new threats and challenges as technology develops. The application of machine learning (ML) and artificial intelligence (AI) has become a viable way to improve cybersecurity measures in recent years. AI and machine learning have demonstrated a great deal of promise for spotting and neutralizing online threats. Through advanced threat detection and prevention in real-time made possible by these techniques, organizations have a greater capacity to assess and handle security incidents [1]. AI and ML can more accurately and efficiently detect patterns, anomalies, and possible threats, reducing risks and adjusting to evolving cyber threats [1]. Threat fishing, which is made possible by AI-powered cyber threat hunting, aims to locate and neutralize malicious entities before they have a chance to harm an organization [1]. AI also enhances the accuracy of malware detection and classification by analyzing vast amounts of security data in real time to promptly identify and address threats [2]. AI and ML can automate threat detection and response processes by spotting patterns in data that might point to possible cyber threats, which minimizes the need for human oversight [2]. Moreover, AI and ML can mimic human intelligence, changing the way we prevent our online premises and generating and gathering cyber threat intelligence [3]. However, there are obstacles and factors to take into consideration when applying AI and machine learning for cybersecurity, including bias, adversarial attacks, explainability, interpretability, data privacy, and security issues[1][3]. Despite these difficulties, machine learning and artificial intelligence offer fascinating opportunities for cybersecurity. For example, self-healing networks are autonomous cybersecurity systems that can recognize, prevent, and reverse the effects of cyberattacks without the need for human assistance [3].

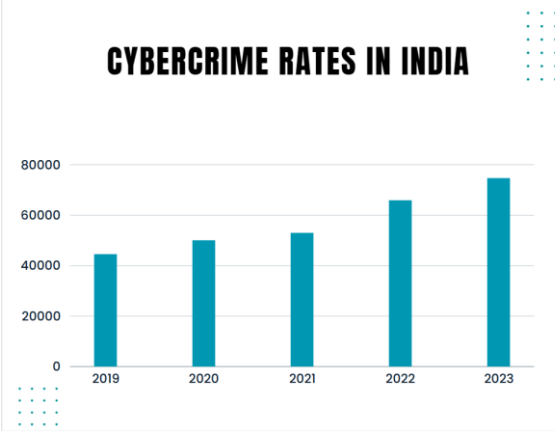

Figure 1:Cybercrime rates in India

India has seen a concerning rise in cybercrime cases in recent years. According to data from the National Crime Records Bureau (NCRB), there were 44,546 cases reported in 2019, which increased to 50,035 in 2020, representing an 11.8% increase. The trend continued in 2021 with 52,974 incidents, marking nearly a 6% increase from the previous year. Unfortunately, the situation worsened in 2022, with a sharp increase in cybercrime cases. The NCRB report shows a total of 65,893 cases registered, representing a substantial 24.4% Increase from the previous year.

A. Ways in which AI and machine learning can enhance security operations and incident response in cybersecurity

AI and ML have demonstrated significant promise in augmenting cybersecurity security operations and incident response. Considering that particular AI applications for cybersecurity are being developed and enhanced, these technologies have an opportunity to yield substantial benefits [4]. AI's capacity to reduce threats to cybersecurity before they arise is one of its most crucial benefits for cybersecurity [4]. AI and ML can detect and categorize malware as well as identify possible threats by examining network traffic [4]. This makes it possible for organizations to prevent cyberattacks and safeguard their sensitive information. AI also helps security experts better analyze, comprehend, and prevent cybercrime, which makes it easier for them to stay up to date with evolving threats [2]. AI and ML have the potential to improve cybersecurity operations and incident response, as well as automate repetitive tasks. This opens up human resources to concentrate on more complex tasks [4]. Organizations may improve client safety and trust while safeguarding their own brand by employing AI and ML to tackle modern cyber threats .[4]. In general, cybersecurity might experience a revolution due to AI and machine learning, which could improve incident response and security operations, automate processes, and identify and stop cyberattacks before they happen. [4].

II. Related work

A. Kirk Bresniker (2019) et al. proposed that the ever-increasing threat landscape highlights the limitations of traditional cybersecurity measures, with frequent and complex attacks posing significant challenges. To bolster defenses, machine learning and artificial intelligence have emerged as valuable tools. However, to truly leverage the potential of AI/ML, it is crucial to understand and identify analyst behavior. The current security approach generates an overwhelming number of alerts, often trivial in nature, making it challenging to collect data on how analysts differentiate between false positives and genuine threats. This challenge comprises five key components. Firstly, standardizing behavior capture of analysts is essential to create a unified data repository for AI/ML model training. Secondly, making cybersecurity activities more engaging and interactive encourages analysts to share their thought processes during simulated attacks, fostering active participation. Thirdly, the distributed nature of network infrastructure presents a challenge, necessitating AI/ML models that can effectively detect threats in complex settings.

B. Harsh Chaudhary(2020) et al. proposed the review of security threats, malware detection, intrusion detection systems, network anomaly detection, attack projection, cybersecurity prediction, and forecasting, the significant role that AI, ML, and DL will play in the field of cybersecurity, and addressing the challenges that the field will face in the future. Artificial Intelligence systems, when given sufficient data, can accurately predict potential cyber-attacks, thus allowing us to prevent them. The emergence of Deep Learning has made this process even more efficient, as it can

effectively handle large datasets. With the abundance of data produced by IT and network systems every second, gathering enough data to create effective Neural Networks has become a simpler task. This paper delves into the application of AI-based systems in identifying cyber attacks and reviews past research in this area. It also discusses how cybersecurity can safeguard AI from attacks that aim to target its decision-making process and the accuracy of AI models.

C. Kamran Shaukat(2020) et al. proposed a concise summary of how machine learning techniques are used in cyber security. It explains the main machine learning techniques employed to detect and classify cyberattacks such as intrusion detection, malware detection, and spam detection, on both computer networks and mobile devices. The article also discusses the recent progress made in machine learning models in the past decade and the difficulties posed by different types of cyber threats. It stresses that each cyberattack is unique and requires a specific approach to address it effectively. Additionally, the article covers fundamental aspects of cyber security, including how cyberattacks are classified on mobile devices and computer networks. It also introduces the basics of machine learning, including its foundations, subtypes, and significant techniques, to help beginners gain a better understanding of this field

D. Asmaa Halbouni(2022) et al. proposed and examined intrusion detection systems and explored the types of learning algorithms utilized by machine learning and deep learning to safeguard data from malicious activities. It delves into recent work in machine learning and deep learning in various network implementations, applications, algorithms, learning approaches, and datasets to create an effective intrusion detection system. Choosing an appropriate dataset to train and test an intrusion detection system is a vital factor, and it is evident that datasets have an effect on research in this field, as some consider them outdated or contain duplicate information. Consequently, the study compares the most commonly used datasets in threat detection over the past decade.

E. Yang Xin(2018) et al**.** proposed machine learning and deep learning methods for network analysis of intrusion detection aiming to provide an overview of the current research in this field. With the increasing integration of the Internet and social life, cybersecurity is becoming a significant concern. The paper focused on machine learning (ML) and deep learning (DL) techniques used for network security and intrusion detection. The review covers the commonly used datasets, challenges, and research directions in ML/DL-based intrusion detection systems. Misuse-based, anomaly-based, and hybrid techniques were discussed, and their pros and cons were highlighted. This also provides a brief tutorial description of each ML/DL method, including decision trees, k-nearest neighbor, artificial neural networks, and support vector machines It covers ML and DL techniques and applications of each method in network intrusion detection

F. Xavier A. Larriva-Novo(2020) et al. propose to delves into the role of artificial intelligence algorithms in cybersecurity and the detection of attacks. It emphasizes the growing use of machine learning algorithms, such as neural networks, for intrusion detection, which can produce superior results in certain situations compared to traditional intrusion detection systems. The study focuses on evaluating different established machine learning algorithms that are often employed in IDS scenarios. To accomplish this, the researchers first categorize cybersecurity data sets into several groups and use this division to determine which neural network model (multilayer or recurrent), activation function, and learning algorithm yield better accuracy values, depending on the data group. Ultimately, the results are used to identify the most relevant and representative group of data for intrusion detection and the most suitable configuration of the machine learning algorithm to reduce the system's computational load. The author concludes by presenting the findings and conclusions of this study, underscoring the significance of machine learning algorithms in cybersecurity and their potential for optimized intrusion detection.

G. Ansh Bilimoria(2021) et al. proposed that the exponential growth of cyber-attacks on

computer infrastructure and personal computers has raised serious concerns about the privacy and security of computer networks. Intrusion detection and prevention systems have emerged as a significant component of cyber security to mitigate this problem. However, the selection of the appropriate technique to use for a given scenario remains a challenge. In this author presents a comparative study of different proposed models for intrusion detection and prevention systems, which utilize machine learning algorithms to attain better performance, and accuracy, and enhance cyber security. The author provides a detailed overview of the classification of IDS into four types: Network-based, Host-based, Perimeter, and VM-based. It also explains the three methods of intrusion detection in IDS/IPS, namely, Signature/Misuse based detection, Anomaly-based detection, and Hybrid. The paper further discusses the most employed dataset in network intrusion detection, namely, the NSL-KDD dataset. The different types of attacks detected in cybersecurity are discussed, including DoS, R2L, U2R, and Probe. This also provides insights into the seven steps involved in implementing a basic IDS using machine learning methods. These steps include loading the dataset, preprocessing, classifying features according to the attacks, applying feature subset selection measures, selecting the best feature subset, applying the classifier, and recording results.

H. Eva Rodríguez et al. proposed that the widespread use of mobile devices and the increasing popularity of mobile services have raised serious cybersecurity challenges. Conventional cybersecurity systems do not ensure the protection of user privacy and have proven incapable of identifying sophisticated attacks and unidentified malware. As a result, Deep Learning (DL) models have gained popularity in cybersecurity systems due to their ability to accurately and efficiently detect new attacks. This paper provides an extensive overview of current cybersecurity research using deep learning in wireless and mobile networks. It covers every facet of cybersecurity, including software attacks, infrastructure attacks and threads, and privacy protection. The author provides a detailed overview of DL techniques applied, or with potential applications, to cybersecurity. It then reviews cybersecurity works based on DL. Each cybersecurity threat or attack, it discusses the challenges of using DL methods. For each contribution, it reviews the implementation details and the performance of the solution. The paper identifies the most effective DL methods for the different threats and attacks and constitutes the first survey that provides a complete review of the DL methods for cybersecurity.

III. Applications of AIML in Cybersecurity

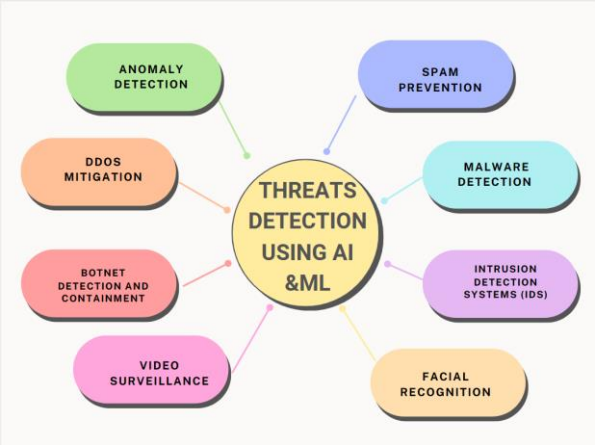

Figure 2: Threat detection using AI and ML

There are various types of threat detection using AI& ML like malware detection, spam prevention, anomaly detection, IDS, etc as shown in the figure.

A. How can artificial intelligence (AIML) improve cybersecurity threat detection and prevention?

In recent years, the application of AIML in cybersecurity has increased in significance. Artificial intelligence and machine learning can detect threats in real time by analyzing huge amounts of data, which can help prevent cyberattacks. Organizations can quickly and effectively detect and address cyber threats due to AIML's capacity to recognize anomalies and patterns that might point to potential dangers [9][10]. Hackers may defeat conventional safety measures and algorithms by focusing on the data that they have been trained to recognize and

the warning signs that they search for [9]. On the other hand, attackers can be found and stopped before they have a chance to harm an organization by utilizing AI-enhanced threat identification and mitigation [11]. One new use of AI and ML in cybersecurity is AI-powered cyber threat hunting [11]. AIML seeks to support cybersecurity systems in modifying unusual threats and vulnerabilities by recognizing and countering sophisticated threats that have avoided conventional security measures [11]. Threat detection and prevention systems can respond to cybersecurity threats more dynamically and proactively through AIML's automation and real-time analysis, which improves their accuracy and efficiency [11]. Machine learning algorithms are used by intrusion detection and prevention systems to examine network traffic and find anomalies, including patterns that correspond to a specific kind of attack [11][12]. To allow up experts to work on more difficult tasks, AIML can automate some aspects of threat detection and response [12]. Moreover, AIML's threat detection skills can be enhanced by training it on cybersecurity data that already exists [12].

B. *What are the specific use cases of AIML in network security and intrusion detection?*

AIML has shown to be a useful tool for intrusion detection and network security. AI-driven security for endpoints defines standards for normal endpoint behavior. It detects errors, enabling the system to differentiate between legitimate and fraudulent behaviors to prevent phishing and malware attacks [13]. By identifying patterns and anomalies, machine learning algorithms can detect and resolve security breaches. These findings may then enhance user account safety and password protection via advanced authentication methods [13]. Network behavior analysis, which examines network traffic to find unusual events or modifications in system behavior, can benefit from the application of AI. This is achieved by looking for patterns in network traffic that point to specific kinds of attacks. Future security measures can be improved by using these patterns to prevent potential dangers with similar features [12]. AIML can detect possible dangers in network security and intrusion detection, analyze malware based on its essential properties, and determine whether a piece of software is intended to remove or encrypt data without permission [14]. In addition, network traffic is analyzed by machine learning algorithms to find anomalies that might point to a possible intrusion [12]. AIML is capable of being trained to identify patterns associated with illegal access attempts, spot a sharp increase in traffic coming from a particular IP address, and check the network as a whole for vulnerabilities. In order to improve network security, AI can also suggest security guidelines, group functional tasks into groups, and identify trends in network traffic [10].[15]. Lastly, network security inspection and vulnerability management utilize AIML. Both of these procedures can be automated by machine learning algorithms, which will increase their effectiveness and efficiency [11]. It should be remembered, however, that AI is a tool that needs human intervention. When AI makes mistakes, humans must get involved. However, improving IT security performance at the corporate level is the primary AI use case in cybersecurity [12][16].

C. *How can AIML be used to improve security analytics and incident response?*

An organization's overall security position can be greatly enhanced by utilizing AIML in incident handling and security analytics. AI-powered solutions may accelerate incident response times by offering more information for prioritizing tasks and responding to security alerts [9]. AI can also assist in identifying the root causes and weak points in an organization's infrastructure, enabling proactive mitigation efforts and preventing further security problems [9]. Additionally, AIML can improve database vulnerability management, allowing organizations to safeguard themselves before recognized danger reporting and patching occurs [15]. By incorporating behavior analysis, UEBA tools powered by AI can identify anomalies pointing to unknown attacks, evaluate user behavior on servers, and enhance threat hunting [15]. AIML has the ability to create individuals of each application operating on a network within an organization, recognize potential breaches, and spot departures from established standards by examining data from multiple sources,

including endpoints [15]. By providing real-time threat information to improve incident response, the application of AIML can also help organizations comprise and investigate incidents more quickly [10][11]. AI can also be used in security operations centers (SOCs) to automate repetitive tasks, freeing up human resources to work on more crucial security-related tasks [11]. Artificial intelligence (AI) real-time analysis allows for instant action in a matter of minutes as opposed to hours or days with manual methods. As a result, attacker opportunities may be reduced, and the possible consequences of a security breach may be limited [10]. In the end, AI can enhance security analytics and incident handling by supporting vulnerability detection and management, supporting in the identification of vulnerabilities in systems and applications, and examining the infrastructure of a company for potential flaws and configuration errors. According to IBM research, AI may reduce the time it takes for organizations to recognize and react to cyber threats by up to 14 weeks [10]. This can be achieved by automating security tasks with AIML.

D. *How can AI and machine learning be used for anomaly detection in network traffic?*

Anomaly detection and network traffic analysis can be done with AI and ML. They streamline the process of detecting network threats by analyzing network behavior to spot anomalies or security incidents that deviate from the norm [1][2]. AI and ML can be used to identify patterns of network activity that point to a particular kind of attack, enabling an analysis-based quick response [1]. Machine learning algorithms are employed to examine network data and identify irregularities, like abrupt surges in traffic originating from a particular IP address [1]. One of the popular security uses for AI and ML is anomaly detection in network traffic, which can improve network defense against anomalies.[2][3]. Furthermore, since AI and ML can eventually learn to recognize and adapt to new threats, future security measures might be strengthened by thwarting possible threats with similar characteristics [2][1]. To create precise anomaly detection systems, machine learning models can be trained on huge amounts of known infections [3]. Moreover, AI can spot anomalous activity in network traffic that might not set off alarms, and systems built on rules can be employed to analyze network traffic behaviorally [1]. In order to spot threats that are disguised and to detect changes from accepted norms, AI may also track both system and user behavior [2][1]. In general, network traffic data can be automatically analyzed by AI and machine learning to detect and react to threats instantly [1].

IV. Research methodology

The research methodology of this paper is designed to investigate the application of Artificial Intelligence and Machine Learning in cybersecurity. The study aims to understand how AI and ML can improve intrusion detection, network security, security analytics, and incident response. To achieve this, the research process involves a comprehensive literature review of academic articles, reports, and books related to this field and it is based on a comprehensive literature review of academic articles, reports, and books related to the application of AI and ML in cybersecurity. The study aims to investigate the benefits and limitations of AI and ML in cybersecurity and understand how they can improve intrusion detection, network security, security analytics, and incident response. To achieve this, the research process involves searching and reviewing relevant academic literature, summarizing and synthesizing key findings, and analyzing the data to draw meaningful conclusions. The literature review comprises a critical analysis of the current state of research in this field, including the latest trends, developments, and applications of AI and ML in cybersecurity. The study identifies the benefits of AI and ML in cybersecurity, such as improved threat detection and response, reduced risks, and automated processes. Additionally, the study highlights the obstacles and factors to take into consideration when applying AI and ML for cybersecurity, including bias, adversarial attacks, explainability, interpretability, data privacy, and security issues.

The research methodology of this paper provides a comprehensive and reliable analysis of the application of AIML in cybersecurity.

The study provides valuable insights into the benefits and limitations of AI and ML in cybersecurity, which can guide further research and help improve cybersecurity measures in the future.

V. Conclusion

The field of cybersecurity is constantly evolving with the emergence of new technologies and the rise of sophisticated cyber threats. As such, there is a growing interest in the use of machine learning (ML) and artificial intelligence (AI) to enhance cybersecurity operations. This research paper aims to explore the specific applications of AIML in cybersecurity and how these technologies can improve threat identification, mitigation, and response. The study posits that AI and ML have demonstrated significant promise in augmenting cybersecurity security operations and incident response. By examining network traffic and categorizing malware, these technologies can help prevent cyberattacks and safeguard sensitive information. Additionally, AI can assist security experts in analyzing, comprehending, and preventing cybercrime, which allows them to stay up-to-date with evolving threats. Furthermore, the research paper emphasizes that the automation of threat detection and response processes by AI and ML minimizes the need for human oversight. This not only saves time and resources but also enables organizations to respond to threats in real-time, reducing the risk of damage. However, the study acknowledges that there are obstacles and factors to consider when applying AI and ML to cybersecurity, including bias, adversarial attacks, explainability, interpretability, data privacy, and security issues.

The paper concludes that despite these difficulties, machine learning and artificial intelligence offer fascinating opportunities for cybersecurity. For example, self-healing networks are autonomous cybersecurity systems that can recognize, prevent, and reverse the effects of cyberattacks without human assistance. By understanding the advantages and limitations of AIML in cybersecurity, organizations can better evaluate the benefits of these technologies and use them to strengthen their cybersecurity protocols.

This study contributes to the growing body of literature on the application of AIML in cybersecurity and offers guidance for further research. As cybercrime rates continue to rise, it is crucial to explore the potential of AI and ML in cybersecurity and invest in the development of these technologies to protect individuals, businesses, and countries from potential cyberattacks. Future research must concentrate on overcoming the limitations and gaps present in the study, while also recognizing the potential weaknesses and biases that may arise from the use of AI and ML in the realm of cybersecurity. Hence, the upcoming research should strive to identify and tackle any potential weaknesses that may arise in the implementation of AIML in cybersecurity, while also exploring novel applications and advancements in this domain.

References

1. *R. Das and R. Sandhane, "Artificial intelligence in cyber security," in Journal of Physics: Conference Series, vol. 1964, no. 4, p. 042072, Jul. 2021.*
2. *Z. Zhang, H. Al Hamadi, E. Damiani, C. Y. Yeun, and F. Taher, "Explainable artificial intelligence applications in cyber security: State-of-the-art in research," IEEE Access, vol. 10, pp. 93104-93139, 2022.*
3. *F. Zhang, X. Cui, Z. Wang, S. Chen, Q. Liu, and C. Liu, "A Systematic Study of AI Applications in Cybersecurity Competitions," in *2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE)*, pp. 138-146, Dec. 2020.*
4. *R. Das and R. Sandhane, "Artificial intelligence in cyber security," in *Journal of Physics: Conference Series*, vol. 1964, no. 4, p. 042072, Jul. 2021.*
5. *K. Bresniker, A. Gavrilovska, J. Holt, D. Milojicic, and T. Tran, "Grand challenge: Applying artificial intelligence and machine learning to cybersecurity," *Computer*, vol. 52, no. 12, pp. 45-52, 2019.*
6. *H. Chaudhary, A. Detroja, P. Prajapati, and P. Shah, "A review of various challenges in cybersecurity using artificial intelligence," in *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, pp. 829-836, Dec. 2020.*
7. *K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, "A survey on machine learning techniques for cyber security in the last decade," *IEEE Access*, vol. 8, pp. 222310-222354, 2020.*
8. *Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "Machine learning and deep learning approaches for cybersecurity: A review," *IEEE Access*, vol. 10, pp. 19572-19585, 2022.*
9. *Y. Xin et al., "Machine learning and deep learning methods for cybersecurity," *IEEE Access*, vol. 6, pp. 35365-35381, 2018.*
10. .
11. *X. A. Larriva-Novo, M. Vega-Barbas, V. A. Villagrá, and M. S. Rodrigo, "Evaluation of cybersecurity data set characteristics for their applicability to neural networks algorithms detecting cybersecurity anomalies," *IEEE Access*, vol. 8, pp. 9005-9014, 2020.*

12. *P. Parkar and A. Bilimoria, "A survey on cyber security IDS using ML methods," in *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*, pp. 352-360, May 2021.*

13. *E. Rodriguez, B. Otero, N. Gutierrez, and R. Canal, "A survey of deep learning techniques for cybersecurity in mobile networks," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1920-1955, 2021.*
14. *R. Calderon, "The benefits of artificial intelligence in cybersecurity," *Revista Espanola de Documentacion Cientifica*, vol. 15, no. 4, pp. 42-66, 2019.*
15. *L. Chan, I. Morgan, H. Simon, F. Alshabanat, D. Ober, J. Gentry, et al., "Survey of AI in cybersecurity for information technology management," in *2019 IEEE technology & engineering management conference (TEMSCON)*, pp. 1-8, Jun. 2019.*
16. *N. Wirkuttis and H. Klein, "Artificial intelligence in cybersecurity," *Cyber, Intelligence, and Security*, vol. 1, no. 1, pp. 103-119, 2017.*
17. *S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, "Harnessing artificial intelligence capabilities to improve cybersecurity," *IEEE Access*, vol. 8, pp. 23817-23837, 2020.*

18. *R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Information Fusion*, p. 101804, 2023.*
19. *D. Sontan and S. V. Samuel, "The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities," *World Journal of Advanced Research and Reviews*, vol. 21, no. 2, pp. 1720-1736, 2024.*
20. *Shah, "Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats," *Revista Espanola de Documentacion Cientifica*, vol. 15, no. 4, pp. 42-66, 2021.*